МВС України
Харківський національний університет внутрішніх справ
Кафедра інформаційних технологій

ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ДІЯЛЬНОСТІ НПУ

Матеріали
науково-практичного семінару

м. Харків, 21 грудня 2018 року

Харків
2018

УДК [351.74:004] (477)(08)
ББК 67.9(4УКР)301.163я43
Н 34

ОРГКОМІТЕТ:

голова – ректор генерал поліції третього рангу Сокуренко В.В.;

заступник голови – перший проректор підполковник поліції Швець Д.В.;

секретар – старший викладач кафедри інформаційних технологій факультету № 4 Рог В.Є.;

члени оргкомітету:

- декан факультету № 4 підполковник поліції Марков В.В.;
- начальник редакційно-видавничого відділу підполковник поліції Білоус П.О.;
- начальник відділу організації наукової роботи підполковник поліції Мірошниченко О.С.;
- начальник відділу матеріального забезпечення Копаниця О.В.;
- начальник інформаційно-технічного відділу Полховський О.М.;
- начальник відділу зв'язків з громадськістю Щербакова І.В.;
- директор загальної бібліотеки Процких Т.О.;
- завідувач кафедри інформаційних технологій факультету № 4 Струков В.М.;
- заступник начальника відділу організації служби Тарасенко В.М.

Друкується за рішенням оргкомітету відповідно до доручення Харківського національного університету внутрішніх справ від 29 листопаду 2018 року

Застосування інформаційних технологій у діяльності НПУ : матеріали наук.-практ. семінару (м. Харків, 21 грудня 2018 р.) / МВС України, Харк. нац. ун-т внутр. справ. Харків. ХНУВС, 2018. 100 с.

У збірнику висвітлено погляди науковців та практиків щодо актуальних питань розробки, впровадження і використання компонентів інформаційних технологій в діяльності правоохоронних органів, проблем підготовки кадрів для інформаційно-аналітичних підрозділів НПУ.

ЗМІСТ

УДК 351.741:004.89 (477)
ВАЛЕРІЙ ВАСИЛЬОВИЧ СОКУРЕНКО
доктор юридичних наук, професор, ректор Харківського національного університету внутрішніх справ, генерал-поліції третього рангу

ТЕХНОЛОГІЇ ТА ІНСТРУМЕНТАЛЬНІ ЗАСОБИ СУЧАСНОГО КРИМІНАЛЬНОГО АНАЛІЗУ

Злочинність може загрожувати безпеці і стабільності як усередині держави, так і на транскордонному рівні. Рада міністрів ОБСЄ неодноразово підкреслювала, що злочини не тільки порушують безпеку окремих осіб, а й здатні привести до більш масштабних конфліктів і насильства. Визнаючи загрозу, яку злочини несуть для безпеки окремих людей, а також їх здатність дати поштовх більш масштабним конфліктам і насильству, держава зобов'язується приймати ряд заходів по боротьбі з цим явищем.

Держава чітко розуміє, що збір і зберігання достовірних даних і статистики про злочини життєво необхідні для формулювання ефективної політики і виділення належних ресурсів на протидію злочинності. Визнаючи потребу в більш послідовних, всеосяжних і придатних для зіставлення даних про злочини, держава зобов'язується «збирати, зберігати і оприлюднити достовірні відомості і досить докладні статистичні дані про злочини, включаючи число випадків, доведених до відома правоохоронних органів, кількість порушених справ і винесених вироків». Загальною метою будь-якої системи збору даних про злочини є не тільки надання особам і органам, відповідальним за формування політики, інформації, яка необхідна їм для того, щоб вони могли приймати добре обґрунтовані рішення і розробляти якісні заходи реагування, а й формування необхідної доказової бази в кожному конкретному випадку для найбільш ефективного і якнайшвидшого відновлення порушених прав своїх громадян або їх об'єднань, які декларуються державою як пріоритет внутрішньої політики.

З огляду на неоднорідність технологічних ланцюжків процесуальних дій і слабку формалізацію первинних документів, держава в особі правоохоронних органів отримує величезний масив як структурованих даних (з чіткою, заздалегідь заданою внутрішньою структурою), так і неструктурованих - інформацію, яка не має певної структури, або здебільшого не організована в установленому порядку. Такі дані, як правило, представлені у формі тексту, який може містити дати, цифри, факти і адресні посилання на нетекстові сховища. Формування осмислених висновків з аналізу такого масиву цілком і повністю лягає на людину.

Разом з тим, поява технології обробки великих даних (Big Data) в кінці 2000-х років стимулювало підвищений інтерес до програм для аналізу неструктурованих даних в сучасних областях, таких як прогнозування і причинно-наслідковий аналіз. Основна концепція програмних продуктів - візуалізація великих масивів даних з різнорідних джерел, що дозволяє користувачам без технічної підготовки знаходити взаємозв'язки між

об'єктами, виявляти збіги між об'єктами і подіями навколо них, виявляти аномальні об'єкти - Data Mining з упором на інтерактивний візуальний аналіз в дусі концепції посилення інтелекту. Як джерела таке програмне забезпечення використовує як традиційні бази даних та інші структуровані джерела, так і тексти, аудіо, відео. При цьому вважається, що для безпосереднього використання продуктів організаціям-замовникам не потрібно персонал з інженерними або програмістські навичками, оскільки вся робота ведеться в інтуїтивному графічному інтерфейсі, а запити до джерел формулюються на природній мові.

В таких умовах є абсолютно необхідним застосовувати для обробки доступної інформації більш ефективні наукоємні системи, зокрема, системи, в яких використовуються технології Data Mining, Visual Mining, Web Mining, Text Mining. Аналіз існуючих автоматизованих інструментальних засобів кримінального аналізу свідчить про те, що в Україні відсутні ефективні засоби автоматизованого кримінального аналізу великих масивів даних, в світі існують певні аналітичні системи (Palantir, I2, ANACAPA, CRIMEVIEW Server, My Neighborhood Map System, CRIMEDC, Holms2), кожна з яких має свої переваги і недоліки, але жодна з них не охоплює повною мірою рішення задач кримінального пошуку та кримінального дослідження з використанням геоінформаційних засобів в реальному часі.

Більшість цих систем пропонують рішення для інформування громадськості та, що принципово важливо, йдеться не про інтеграцію в уже діючі системи, а установку їх як незалежних систем. Найбільш ефективними і поширеними з перелічених систем є Palantir (США), I2 (фірма IBM), Holms2 (Великобританія). Palantir використовується в ЦРУ, АНБ, ФБР, поліцейських управліннях Нью Йорка, Лос Анджелеса, банку JP Morgan. В I2 дуже обмежено використовуються геоінформаційні технології. Holms2 використовується лише у Великобританії.

Проведенній аналіз свідчить, що існує нагальна потреба забезпечення фахівців, що займаються кримінальним аналізом, системами, які здатні проводити обробку великих масивів неструктурованих даних саме в автоматизованому режимі з використанням вже накопичених даних. В даний час більшість систем кримінального аналізу створені за кордоном і не враховують повною мірою особливості кримінального процесу в Україні. Таким чином, необхідно забезпечити кримінальних аналітиків ефективним інструментарем, який буде ґрунтуватися на наступних принципових моментах: 1) урахування особливостей масивів даних, що обробляються, 2) забезпечення можливості просторового візуального аналізу, 3) інструментарій повинен бути виконаний як надбудова (оболонка) існуючої ІПНПУ, що дозволить при його впровадженні не видаляти стару систему або припиняти її функціонування, а просто і безболісно істотно поліпшувати її функціональність і ефективність.

УДК 004.735

СЕРГІЙ ВАСИЛЬОВИЧ ДЕМЕДЮК
Начальник Департаменту кіберполіції Національної поліції України
генерал поліції третього рангу
В'ЯЧЕСЛАВ ВАЛЕРІЙОВИЧ МАРКОВ
кандидат юридичних наук, доцент, начальник факультету № 4
Харківського національного університету внутрішніх справ
підполковник поліції

ДИСТАНЦІЙНЕ НАВЧАННЯ В СИСТЕМІ ПІДГОТОВКИ КАДРІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Глобальна інформатизація суспільства на рубежі 21 сторіччя, яка є результатом розвитку інформаційних і телекомунікаційних технологій, придбала характер "інформаційної революції" та радикально змінила роль і місце інформації в сучасному суспільстві.

Останні досягнення у галузі нових інформаційних технологій (НІТ) (включаючи появу персональних комп'ютерів, створення глобальної комп'ютерної мережі Інтернет, розвиток технологій мультимедіа, гипермедіа, віртуальної реальності й ін.) значно впливають і на сферу надання освітніх послуг та підготовки кадрів для національної поліції. Їхнє використання дозволяє підвищити ефективність навчання і рівень кваліфікації співробітників поліції, а також сприяти впровадженню НІТ у практичну діяльність національної поліції та формуванню системи відповідного інформаційного забезпечення, метою якої є всебічна інформаційна підтримка діяльності поліції у боротьбі зі злочинністю в Україні.

НІТ дозволяють удосконалювати механізми керування системою підготовки кадрів; удосконалювати методологію і стратегію відбору змісту, методів і організаційних форм навчання, що відповідають задачам підготовки фахівців для інформаційного суспільства; створювати методичні системи навчання, що реалізують принцип самостійного творення знань та є орієнтованими на розвиток інтелектуального потенціалу слухача, підвищення його рівня самостійності та здібностей до самонавчання.

З'являються нові форми представлення навчального матеріалу, нові форми доступу до нього, нові можливості в моделюванні процесів і явищ, що досліджуються, нові форми організації взаємодії курсантів з викладачем і усередині групи, нові різновиди педагогічних програмних систем, яки містять інформацію про деяку предметну галузь, реалізують технологію її вивчення та створюють умови для виконання різних видів навчальної діяльності.

До основних методичних цілей, яки найбільш ефективно реалізуються за допомогою таких програмних засобів можна віднести наступні [1]:

– індивідуалізація і диференціація навчання;

– формування культури навчальної діяльності, у т.ч. інформаційної;

– розвиток інтелектуального потенціалу курсантів та підвищенні їх мотивації;

– формування навичок прийняття рішень у складних ситуаціях;
– здійснення контролю і самоконтролю за процесом навчання;
– комп'ютерне моделювання процесів і явищ;
– якісно більш високий ступінь візуалізації навчального матеріалу за рахунок використання технології мультімедіа, гіпермедіа та віртуальної реальності;
– реалізація доступу до інформаційних ресурсів поза залежністю від місця їх розташування, який здійснюється на основі технологій телекомунікації.

Однією з найперспективніших технологій, яка дозволяє ефективно впроваджувати новітні інформаційні технології у систему підготовки кадрів для Національної поліції є дистанційне навчання (ДН).

ДН є системою надання освітніх послуг, що передбачає широке використання нових інформаційних технологій для доступу слухачів до освітніх ресурсів та їхньої активної взаємодії з викладачами й колегами в процесі роботи з навчальним матеріалом.

До основних системоутворюючих характеристик ДН можна віднести:

1. Просторовий та/або тимчасовий поділ учасників освітнього процесу протягом більшої його частини.

2. Використання певних інформаційних технологій для подання навчального матеріалу та доступу до нього.

3. Реалізація можливості двостороннього зв'язку слухача з установою, що надає освітні послуги, викладачем й іншими слухачами.

ДН можна розглядати як форму навчання, яка йде на зміну заочній формі, створює більше комфортні умови для навчання та дозволяє досягти більш високих результатів. Досягається це за рахунок інтенсивного використання можливостей нових інформаційних технологій (насамперед комп'ютерних технологій подання й обробки інформації, а також мережевих технологій телекомунікації).

Сучасні комп'ютерні технології подання інформації (мультимедіа, гипермедіа, відео й аудіо технології, анімація, 3D-графіка й ін.) дозволили розробляти курси ДН з якісно більше високим ступенем візуалізації й організації навчального матеріалу. Мережні технології телекомунікації (електронна пошта, IRC, комп'ютерні аудіо та відеоконференції) кардинально розширили можливості взаємодії слухачів з викладачем і своїми колегами в процесі вивчення матеріалу. Сучасний комп'ютерний курс ДН є високоінтерактивним навчальним середовищем, що надає слухачеві доступ до навчальних ресурсів і можливість інтенсивної й різноманітної взаємодії з іншими учасниками освітнього процесу.

На цей момент розроблені та активно використовуються кілька моделей ДН, які розрізняються цілями, завданнями, технологіями, організацією освітнього процесу, цільовою аудиторією й взаємодією організацій, що надають освітні послуги.

Найбільш значимими властивостями, що визначають великий потенціал використання ДН в системі підготовки й підвищення кваліфікації співробітників національної поліції, є наступні:

4. Навчання може здійснюватися без відриву від основної діяльності, що дозволяє уникнути проблем, пов'язаних з перерозподілом службових обов'язків співробітника на час його відряджень.

5. Слухачі можуть працювати з матеріалом у зручний для себе час, у зручному темпі, за зручним для себе розкладом.

6. Кожен слухач має швидкий і зручний доступ до всіх необхідних освітніх ресурсів.

7. Організація отримує значну економію коштів у зв'язку з відсутністю необхідності оплати відрядних витрат, проживання й проїзду співробітника до місця навчання.

8. Комп'ютерні дистанційні курси можуть легко створюватися та модифікуватися у відповідь на реальні потреби тих або інших організацій і служб.

Ефективність функціонування системи ДН визначається цілим рядом організаційних, адміністративних, технологічних та інших факторів.

Зараз існує безліч класів педагогічних програмних систем, що розрізняються за призначенням, за реалізованими моделями навчання та технологіям презентації навчального матеріалу, його доставки та організації взаємодії зі слухачем. До таких систем, які на практиці продемонстрували досить високу ефективність, можна віднести комп'ютерні навчальні курси, програми-тренажери, системи тестування і контролю, системи імітаційного моделювання, демонстраційні системи, комп'ютерні підручники та ін.

ДН, особливо його асинхронна форма, широко використовується під час підготовки співробітників поліції різних держав. Наприклад, освітні послуги для підготовки офіцерів поліції у дистанційної формі надають: департамент кримінології університет Лічестера (Великобританія), університет Портсмута (Великобританія), Королівський коледж поліції Нової Зеландії, університет Ліверпуля, Ліцей Преторії (Південноафриканська Республіка), організація Oxbridge Home Learning (Великобританія) та ін. Також під час навчання широко використовуються спеціальні програмні системи. Наприклад, довгий час у Шотландському поліцейському коледжі використовується система VISTRAIN (Video-Based Integrated System for Training Applications), яка дозволяє моделювати та відпрацьовувати дії офіцерів поліції під час деяких інцидентів [2].

В Харківському національному університеті внутрішніх справ також впроваджено ДН для студентів заочної форма навчання. Отримані результати достатньо обнадійливі та дозволяють зробити висновки про перспективність та необхідність подальшого розвитку цього напряму.

Таким чином, широке використання ДН та новітніх інформаційних технологій у системі підготовки і підвищення кваліфікації кадрів національної поліції дозволяє:

– підвищити інтенсивність та якість навчання курсантів;

– впроваджувати в навчальний процес нові перспективні освітні технології і форми навчання;

– сформувати у курсантів і слухачів високий рівень інформаційної культури;

– підвищити мобільність та знизити затратність системи перепідготовки кадрів поліції.

Все це сприяє розв'язанню головного завдання поліції – боротьбі зі злочинністю в Україні.

Список використаних джерел:

1. Чернилевский Д.В., Филатов О.К. Технология обучения в высшей школе.-М.: «Экспедитор», 1996 – 288 с.

2. The VISTRAIN Training System for Police Management of Major Incidents (http://richardmillwood.net/naec/walking-backwards/Vistrain%20training%20system.pdf).

УДК 004.932

ДЕНИС ОЛЕГОВИЧ ПЕФТІЄВ
начальник Управління кримінального аналізу Національної поліції України
ЄВГЕНІЙ ВІКТОРОВИЧ ПАНЧЕНКО
головний інспектор 3-го відділу Управління кримінального аналізу Національної поліції України, аспірант заочної форми навчання Національної академії внутрішніх справ

ЗАСАДИ ПОБУДОВИ ЕФЕКТИВНОЇ СИСТЕМИ ВІДЕОНАГЛЯДУ (ЕТАПИ ТА СУБ'ЄКТИ РЕАЛІЗАЦІЇ)

Актуальність обраної теми формує дві складові, що є дзеркалом сучасності, з одного боку – це глобалізація суспільства, що розпочалася зі зміни світового устрою (розвитку сервісної складової у діяльності населення), розбудови мегаполісів та відповідно збільшення кількості населення, яке іммігрує з маленьких містечок до великих міст. З іншого боку, закон Мура який описав тенденції розвитку технологій, і на сьогодні ми маємо можливість оперувати надвеликими масивами даних, опрацьовуючи їх у мільйони разів швидше ніж десять років тому, вартість таких обчислень у свою чергу у тисячи разів зменшилася.

Більшість розвинених країн зрозуміли ситуацію у якому перебуває суспільство, а тому зосередилися на використанні новітніх технологій в управлінській та правоохоронній діяльності. Адаптація вже наявного досвіду розробників інтелектуальних систем, у тому числі відеонагляду допоможе міським службам та правоохоронним органам організувати свою діяльність більш раціонально, спрямовуючи людські ресурси на опрацювання меншого масиву даних отриманих з вулиць. А весь масив інформації, за визначеними

сценаріями буде опрацьовувати інтелектуальна система, у разі порушення алгоритмів буде відбуватися попередження відповідних служб.

Сьогодні розвиток інтелектуальної відеоаналітики відбувається за двома основними технологіями - це трекінг і ідентифікація. На основі правил, закладених в алгоритм відеоаналізу, будується весь функціонал системи, який вкрай необхідний для побудови сучасних систем відеоспостереження. У межах побудови систем «Смарт-сіті» актуальним є кожен з напрямків, трекінг покликаний вирішити питання:

- незаконного перетину об'єктом прямої лінії в заданому напрямку;
- підозрілого руху у визначеній зоні;
- вихід об'єкта із визначеної зони;
- зупинка об'єкта в зоні;
- залишений в зоні предмет.

У свою чергу ідентифікація, тобто розпізнавання образу по відеозображенню, групування за класами або конкретними шаблонами і порівняння із заздалегідь підготовленою базою еталонних зображень найбільше використовується для розпізнавання обличь, розпізнавання автомобільних номерних знаків, а також ідентифікації транспортних засобів (тип, марка, модель, колір).

Зазначений функціонал є базисом для побудови дієвої системи відеонагляду, адже саме його наявність задовільнить потреби правоохоронних органів, комунальних та дорожніх служб. Охоплення завдань, що покладені на різних суб'єктів державної влади дозволить зосередити їх зусилля на досягненні єдиної цілі – побудови дієвої системи інтелектуального відеоспостереження.

Ефективне впровадження системи інтелектуального відеонагляду залежить від керівника обласної державної адміністрації, мера міста, керівника поліції та активної участі інших представників органів влади та громадськості.

Лише за умови плідної співпраці між цими суб'єктами можливо побудувати платформу для комплексного вирішення питань безпеки, боротьбою зі злочинністю, забезпечення реагування на аварії природного та техногенного характеру, координацію сил та засобів усіх служб, оптимізацію процесів в місті, створення комфортних умов для життя та роботи громади.

На прикладі побудови інтелектуальної системи відеонагляду у Донецькій області, можемо виокремити наступних суб'єктів її реалізації:

Відповідно до статті 13 Закону України «Про місцеві державні адміністрації до відання місцевих державних адміністрацій у межах і формах, визначених Конституцією і законами України, належить вирішення питань щодо забезпечення законності, охорони прав, свобод і законних інтересів громадян в регіоні, соціально-економічний розвиток відповідних територій, здійснення державної регуляторної політики, оборонної роботи та мобілізаційної підготовки.

Іншим суб'єктом можуть виступати органи місцевого самоврядування, з огляду на положення Закону України «Про місцеве самоврядування» до їх компетенції також віднесено повноваження у сферах оборони, обслуговування населення, забезпечення безпеки та фінансові повноваження.

Найголовнішим суб'єктом, що має ініціювати проекти у власній області виступає Головне управління поліції у області, управління у місті чи центральні органи поліції, до їх відання можемо віднести наступні елементи:

1. Загальна координація проекту на всіх етапах його реалізації.
2. Підготовка технічного завдання та правове супроводження побудови системи.
3. Пошук приміщення, котре за технічними вимогами буде придатним для розміщення апаратної частини комплексу.
4. Пошук та визначення виконавця проекту, який буде задовольняти мінімально визначені вимоги.
5. Координація зусиль усіх суб'єктів залучених до реалізації.
6. Виділення осіб для навчання та подальшого супроводження діяльності системи (як апаратної, так і програмної частини).
7. Здійснення тестування системи та підготовка пропозицій щодо її вдосконалення (за необхідності).
8. Введення в експлуатацію системи (спільно з виконавцем), розробка принципів обміну інформацією між різними органами (зацікавленими в використанні системи) та в середині поліції.

У результаті чіткого розуміння кожним суб'єктом доцільності побудови інтелектуального відеонагляду, перших результатів можливо досягнути уже за один рік від початку реалізації проекту побудови інтелектуальної системи відеонагляду. У свою чергу, позитивний досвід областей де вже реалізовано схожі проекти, має сформувати впевненість у досягненні результатів щодо зниження рівня злочинності, розвитку систем управління трафіком тощо.

Список використаних джерел:

1. Про місцеві державні адміністрації: Закон України (із внесеними змінами) від 09.04.1999 р. № 586 XIV. Голос України. 2018. с. 9-16

2. Про місцеве самоврядування в Україні: Закон України (із внесеними змінами) від 21.05.1997 № 280/97-ВР. с. 10-18

3. Про Національну поліцію України: Закон України від 02.07.2015 № 580-VIII. с. 6-20

4. Організаційно-правові та організаційно-технічні аспекти використання систем інтелектуального відеоспостереження (СІВС) із функцією відео аналітики при митному спостереженні як однієї із складових митної безпеки: концептуальне визначення базових понять, шляхи й засоби забезпечення та практичної реалізації : звіт про НДР (заключний) / Державний науково-дослідний інститут митної справи ; кер. П. В. Пашко ; викон. Ю. Г. Коваль [та ін.]. – Хмельницький, 2013, – 104 с.

5. Відеоспостереження, спеціалізована відео техніка [Електронний ресурс]. – Режим доступу : http://kaschtan.com.ua/shop/category_23_Videonablyudenie.html

УДК 65.012.8 + 004

ДМИТРО ВОЛОДИМИРОВИЧ ШВЕЦЬ
кандидат педагогічних наук, доцент, перший проректор Харківського національного університету внутрішніх справ

ПРОБЛЕМИ КАДРОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНО-АНАЛІТИЧНИХ ПІДРОЗДІЛІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

На поточний момент система інформаційного забезпечення Національної поліції України проходить складний період реформування. Цей процес визначається переходом на дворівневу організацію підрозділів служби і подальшим впровадженням досягнень у ІТ галузі в діяльність інформаційної служби. В першу чергу це стосується застосуванням хмарних технологій і створення ЦОД (центрів обробки даних), більш широким впровадженням міжвідомчої взаємодії в частині обміну службовими даними, а також широким впровадженням систем відео спостереження. Крім того, постійно триває процес накопичення даних у базах інтегрованої системи Інформаційний портал НПУ (АРМОР). Кількість записів в системі вже тепер налічує десятки мільйонів записів. В той же час принцип обробки даних в системі залишається лінійним – як і в будь-якій інформаційно-пошуковій системі (наприклад, Google). Результатами обробки запитів до системи часто є перелік об’єктів, який налічує тисячі записів. Такі документи в подальшому обробляються суб’єктами запитів вручну, що потребує дуже багато часу і уповільнює процес розслідування. Таким чином, актуальною задачею є застосування не просто інформаційно-пошукових систем, а систем нового покоління – інформаційно-аналітичних, які б скорочували результати запитів до декількох десятків об’єктів.

Реалізація цих новацій потребує відповідного забезпечення кваліфікованими кадрами. І ось в цьому напрямку є певні проблеми державного рівня.

По-перше, вже декілька років як служба перестала отримувати кадрову підтримку з ХНУВС - випускників спеціальності «комп'ютерні науки», які отримували комплексну підготовку - технічну і поліцейську. Інші ВНЗ системи МВС України не здійснювали підготовку фахівців цього профілю. Ці фахівці найбільшою мірою були пристосовані працювати в інформаційно-аналітичних підрозділах органів внутрішніх справ відразу після закінчення вузу як з точки зору мотивації так і з точки зору технічної та поліцейській підготовленості. Зараз випускники ХНУВС цієї спеціальності займають ключові посади провідних фахівців і керівників у більшості обласних інформаційно-аналітичних підрозділів і в Департаменті інформаційно-аналітичної підтримки Національної поліції України.

Таких спеціалістів на сьогодні вкрай не достатньо не тільки на територіальному, а й на регіональному рівні, про що свідчать керівники практично всіх інформаційно-аналітичних підрозділів у регіонах, з якими традиційно науковці ХНУВС підтримують тісні ділові зв’язки. В цьому

переконуються і викладачі, які проводять заняття в рамках підвищення кваліфікації працівників інформаційно-аналітичних підрозділів: посади не тільки інспекторів, а й інженерів-програмістів, особливо на територіальну рівні в деяких випадках займають психологи та учителі російської мови і літератури, а іноді “спеціалісти ” із середньою освітою (11 класів).

По-друге, як відомо, заробітна плата ІТ фахівців у комерційному секторі перевищує заробітну плату фахівців, зайнятих у бюджетній сфері в декілька разів. Природним чином це обумовлює постійний відтік висококваліфікованих ІТ-спеціалістів в приватні структури саме з бюджетних організацій. З чого однозначно випливає, що при нинішньому рівні заробітної плати і умовах служби не доводиться очікувати напливу великої кількості талановитих молодих фахівців із цивільних технічних вузів.

По-третє, фінансування саме розвитку більшості бюджетних організацій (у тому числі і органів внутрішніх справ) в силу відомих причин зараз обмежене. І якщо ФБР мало можливість собі дозволити витратити 1 мільярд доларів тільки на комп’ютерну програму динамічного розпізнавання облич (так само як і китайський департамент фінансового моніторингу), то Депертамент інформаційно-аналітичної підтримки Національної поліції України в основному може розраховувати лише на зарубіжну фінансову підтримку, оскільки основне бюджетне фінансування направлене на реформування поліції.

По-четверетє, підготовка кваліфікованих фахівців в ІТ сфері вимагає наявності викладачів відповідно високої кваліфікації. На поточний момент в цьому напрямку всі ВНЗ, які готують фахівців у ІТ сфері, стикаються з проблемою відтоку молодих кваліфікованих фахівців у комерційні структури за відсутності матеріальної мотивації.

Внаслідок вищенаведених причин на поточний момент підрозділи інформаційно-аналітичної підтримки Національної поліції України відчувають гостру нестачу кваліфікованих кадрів, яка з плином часу лише загострюється. Також слід зауважити, що ІТ підготовка є багатокомпонентною і передбачає досить тривалий термін навчання.

Можливі варіанти подолання позначеної кадрової проблеми:

1) поновлення набору на спеціальність «Комп’ютерні науки» у ХНУВС,

2) як компромісний варіант з точки зору мінімізації бюджетних коштів – поновлення набору на спеціальність «Компютерні науки» у варіанті 2+2: 2 роки навчання за кошти кандидатів (фахова ІТ підготовіка), 2 роки – навчання за бюджетні кошти (поліцейський компонент),

3) запровадження короткострокових (6-9 місяців) курсів перепідготовки для фахівців інформаційно-аналітичних підрозділів на вимогу департамента ДІАП або фахівців інших підрозділів, які мають технічну освіту в галузі ІТ.

УДК 343.9:159.9.075

ДМИТРО ЮРІЙОВИЧ УЗЛОВ
кандидат технічних наук,
начальник Управління інформаційно-аналітичної підтримки ГУ НП в Харківській області, полковник поліції
ВОЛОДИМИР МИХАЛОВИЧ СТРУКОВ
кандидат технічних наук, доцент, завідувач кафедри інформаційних технологій факультету № 4 Харківського національного університету внутрішніх справ

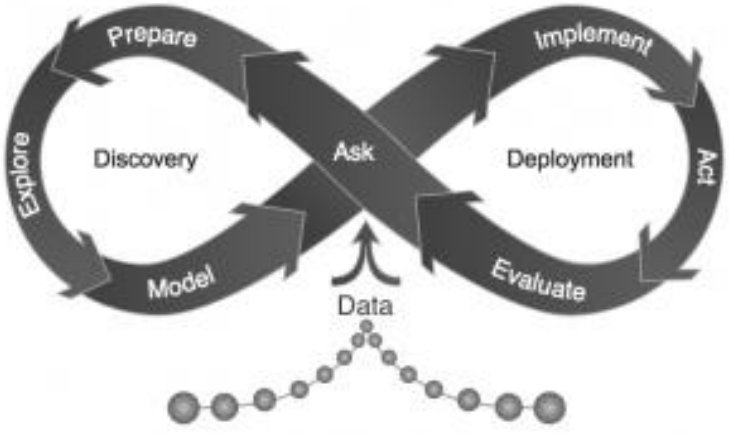
ВИКОРИСТАННЯ МЕТОДІВ І ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ В КРИМІНАЛЬНОМУ АНАЛІЗІ

Основним завданням кримінального аналізу є пошук неочевидних рішень в умовах неповної інформації, що є основною ознакою інтелектуальності. Кримінальний аналіз базується на великих масивах кримінально значимої інформації, яка часто є потоками слабоструктурованих і неструктурованих текстових масивів. Аналіз цієї інформації здійснюється правоохоронцями на основі дедуктивних і індуктивних методів і асоціативного мислення, отже, може бути автоматизований з використанням методів і технологій штучного інтелекту.

Інтелектуальний аналіз кримінальних даних включає в себе такі обов'язкові етапи:

- колекція даних і їх підготовка (препроцесінг);
- класифікація, кластеризація і семантичний розбір підготовлених даних;
- пошук прихованих закономірностей;
- прогнозування;
- візуалізація результатів.

У разі безперервного аналізу в режимі реального часу, інтелектуальний аналіз переходить в циклічний процес з додаванням етапу коригування і уточнення (додавання або зменшення параметрів) вихідних даних.



Мал. 1. Модель Data Mining цикла

1. Колекція даних і їх підготовка (препроцесінг).

На даному етапі відбувається визначення джерел інформації, витяг кримінально значимої інформації, вибір обов'язкових атрибутів, компресія.

Використовуються методи: антиціпаційного алгоритму (схеми передбачення), асоціативні правила, нейронні алгоритми навчання.

На практиці: очищення даних інформаційно-пошукових систем від сміття і перетворення їх в знання, формування метаданих з існуючих баз даних, формування метапошукових запитів в зовнішнє середовище.

2. Класифікація, кластеризація і семантичний розбір.

Дані групуються або за класами (в разі можливості їх визначити заздалегідь), або по кластерам (в разі неможливості їх визначити заздалегідь). Визначається смислове значення даних (семантичний розбір) і будується функція приналежності до того чи іншого класу або кластеру.

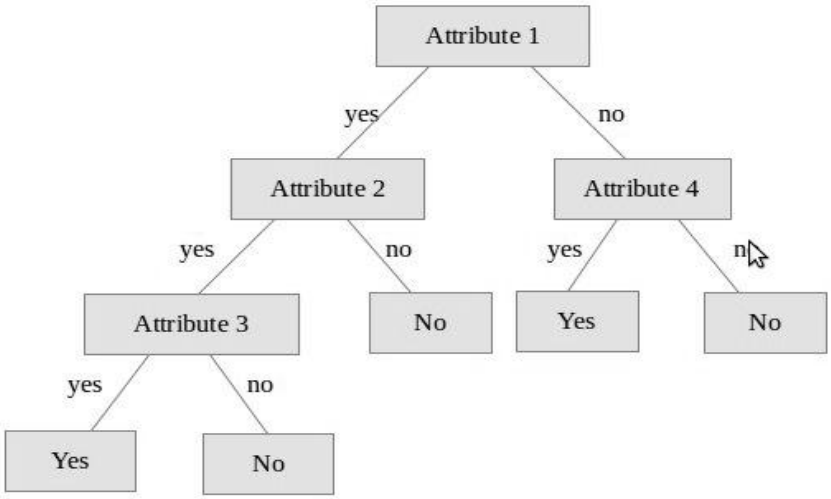
Використовувані методи: Байєсівський алгоритм, регресійний аналіз, K - means, C- means, Fuzzy Logic, латентно-семантичний аналіз, імовірнісний аналіз.

На практиці: угруповання подій за класами і групами; побудова поведінкових профілів подій, об'єктів і суб'єктів; угруповання осіб за поведінковим профілем; виявлення групової та серійної злочинності.

3. Пошук прихованих закономірностей.

Виявляється кореляція між різними процесами і множинами даних. Визначаються взаємодії множин, будуються перетини і відповідності.

Використовуються методи: дерева рішень, кластерний аналіз, нечітка логіка, асоціативна логіка, нейронні мережі, апріорний алгоритм.



Мал. 2 Дерево рішень

На практиці: групування подій за схожими (в т.ч. заздалегідь невідомими) ознаками; визначення множини осіб, відповідній певній групі (кластеру) подій; modus operandi; визначення тенденцій і закономірностей прояву злочинності за локалізацією, часовими та іншими можливими залежностями.

4. Прогнозування.

Визначення ймовірностей і можливостей настання подій в певному місці, в певний час, певним чином.

Використовуються методи: дерева рішень, динамічні ряди, алгоритми нечіткої логіки, теорії ймовірності.

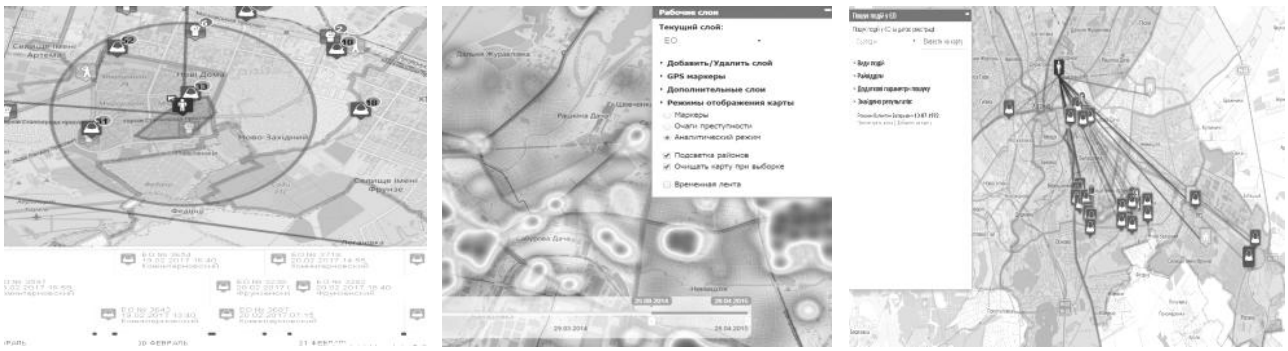
На практиці: визначення місць, часу, обставин, при яких ймовірність скоєння кримінальних подій висока; виявлення циклічних процесів на певній локалізації; виявлення осіб, схильних до вчинення протиправних дій; виявлення ланцюжків обставин, що сприяють вчиненню злочинів.

5. Візуалізація результатів.

Представлення результатів у вигляді, зручному для сприйняття і інтуітивно зрозумілому. Підтримка прийняття рішення на основі відображення множини станів різних індикаторів.

Використовуються методи: crime mapping, OLAP, Visual Mining.

На практиці: візуалізація на електронній карті місць концентрацій різноманітних подій; візуалізація зв'язків подій, осіб, об'єктів, процесів в просторі та часі.



Мал. 3 Приклади візуалізації

Список використаних джерел:

1. Investigative Data Mining for Security and Criminal Detectio. Jesus Mena – Butterworth Heinemann s an imprint of Elsevier Science. Copyright © 2003, Elsevier Science (USA).

2. Whitepaper, "Oracle's Integration Hub For Justice And Public Safety", Oracle Corp. 2004, available at: http://www.oracle.com/industries/government/IntegrationHub_Justice.pdf

3. Прикладний кримінальний аналіз на базі інформаційно-аналітичної системи «RICAS»: методичні рекомендації щодо аналітичної діяльності та кримінального аналізу на базі інформаційно-аналітичної системи «RICAS». Харків : «Юрайт», 2018. 92 с.

УДК 004.056:341.4
КАРЕН ЮРІЙОВИЧ ІСМАЙЛОВ
кандидат юридичних наук, завідувач кафедри кібербезпеки та інформаційного забезпечення Одеського державного університету внутрішніх справ
ВОЛОДИМИР ГЕОРГІЙОВИЧ ПЯДИШЕВ
кандидат технічних наук, доцент, доцент кафедри кібербезпеки та інформаційного забезпечення Одеського державного університету внутрішніх справ

СУЧАСНІ ТЕНДЕНЦІЇ РОЗВИТКУ КІБЕРЗЛОЧИННОСТІ

У світі, керованому соціальними мережами, онлайн-транзакціями, хмарними обчисленнями і автоматизованими процесами, технології розвиваються швидко. Але паралельно з технологічної еволюцією відбувається прогрес кіберзлочинності, яка постійно розвиває нові типи атак, інструменти і методи, що дозволяють злочинцям проникати в більш складні або добре контрольовані середовища, а також збільшувати збитки і навіть залишатися непомітними. Але окрім загального очікування поширення кіберзлочинності, з метою ефективності витрачання ресурсів на боротьбу з нею, необхідно здійснювати більш детальні прогнозування напрямів і масштабів її поширення у різних сферах держаної діяльності, бізнесу, охорони здоров'я тощо. .

Отже, Netwrix – приватна компанія (США) по забезпеченню IT-безпеки, яка пропонує рішення для IT-аудиту для систем і додатків в IT-інфраструктурі, – на підставі аналізу даних 2015 р. визначала напрями, що потребують найбільшої пильності у боротьбі з кіберзлочинністю, таким чином [1]:

1. Злом або шкідливі програми. Шкідливі програми і електронні записи сторонніх осіб залишалися основною причиною порушень даних другий рік поспіль. Зареєстровані випадки сталися через те, що хакери отримали несанкціонований доступ до системи компанії за допомогою атак веб-додатків, шпигунських програм, соціальної інженерії і троянів. Це містить левову частку всіх скомпрометованих даних клієнтів (близько 195 мільйонів записів).

2. Другий найбільш часто зареєстрований тип кіберзлочинності – це несанкціонований доступ до інформації, що зберігається на портативних пристроях, включаючи ноутбуки, смартфони та зовнішні жорсткі диски. Результатом є втрата понад 20 000 конфіденційних даних у 2015 р.

3. Ненавмисне розкриття (людський фактор). Більше 38 000 записів було розкрито через помилки працівників: неправильна адресація електронної пошти та конфіденційної інформації, випадкове розміщення на веб-сайтах компаній.

4. Неправомірна робота інсайдерів (працівників з легальними правами) – порушення цілісності даних:інсайдери заподіяли значної шкоди і скомпрометували більше 600 000 записів клієнтів.

5. Фізичні (неелектронні) втрати даних: втрата або викрадення неелектронних активів з конфіденційною інформацією (паперових документів, карток, канцелярських пристроїв) стали основною причиною витоку даних, що призвело до втрати 1100 записів.

Разом з тим, проведення спеціалізованих досліджень надали можливість встановити важливі кореляції (зв'язки), наприклад, кореляція між видами діяльності і типами атак. Отже, кібер-шпигунство, швидше за все, націлено на уряд, ЗМІ та правоохоронні органи і вельми малоймовірно в інших секторах (роздрібна торгівля, телекомунікації, онлайн-послуги тощо) [2].

Кореляція свідчить також, що, метою кібер-шпигунства, кібервійни і хактівізма швидше за все є державний сектор (уряд, правоохоронні органи, освіта тощо). Проте кібер-злочинність все ж таки націлена на всі сфери бізнесу.

Стосовно динаміки останнього часу щодо поширення проявів кіберзлочинності показові результати лабораторії Malwarebytes Labs, від липня 2018 р. Отже, протягом другого кварталу 2018 р. спостерігалась наступна динаміка проявів кіберзлочинності [3]:

- Cryptomining все ще трималися на високому рівні, але почали знижуватися;
- GandCrab домінували серед програм для вимагання;
- Рекламне програмне забезпечення, що нав'язують, виросло на 19% у порівнянні з попереднім кварталом;
- VPNFilter дебютувало з більш ніж 500.000 виявленнями;
- Експлойти — комп'ютерні програми, що використовують уразливості в програмному забезпеченні та застосовуються для проведення атаки на обчислювальну систему, — демонстрували підйом;
- Шахраї все частіше спрямовували зусилля на PII (особові дані ідентифікації).

Нагадаємо, тут:

- Cryptomining - це вид програми вимагання, яка шифрує всі файли користувача і змінює їх в форматі .KRAB. Вона не блокує використання комп'ютера користуачем, але шифрує практично всі файли на комп'ютері [4].
- GandCrab - це вид програм для здійснення вимагань, які шифрують всі файли користувача і змінюють їх до формату .KRAB, при цьому не блокується використання комп'ютера користувачем, але практично всі файли на комп'ютері шифруються [5];
- VPNFilter — шкідливе програмне забезпечення для зараження маршрутизаторів .
- Експлойти — комп'ютерні програми, що використовують уразливості в програмному забезпеченні та застосовуються для проведення атак на обчислювальну систему;
- PII (personal identification information) — особиста ідентифікаційна інформація.

Висновок.

1. Загальна кількість кібератак у світі розширятиметься.
2. Кібер-шпигунство, кібервійна і хактівізм атакуватимуть у першу чергу державний сектор (уряд, правоохоронні органи, освіта тощо).
3. Основна маса порушень і компрометації даних, як і раніше, здійснюватиметься через використання шкідливих програм, причому

об’єктами злому все частіше будуть портативні пристрої, а також побутові системи типу «розумний будинок», тощо.

4. Значною проблемою у протистоянні кіберзлочинності залишатиметься кримінальна діяльність «інсайдерів».

5. Кіберзлочинці все більше уваги приділятимуть приховуванню слідів своєї злочинності.

Список бібліографічних посилань:

1. Irvine, C.A. Top five cybercrime patterns to watch out for in 2016. *Netwrix, January 5, 2016*. URL : https://www.netwrix.com/ top_five_cybercrime_patterns_for_2016.html [Accessed 25 November, 2018].

2. Bendovschi A. Cyber-Attacks – Trends, Patterns and Security Countermeasures. *Procedia Economics and Finance, Volume 28, 2015, Pages 24-31* : site. URL : https://www.sciencedirect.com/science/article/pii/ S2212567115010771#! [Accessed 25 November, 2018].

3. Cybercrime tactics & techniques Q2 2018. Malwarebytes Labs. July 23, 2018 : site. URL : https://blog.malwarebytes.com/malwarebytes-news/ctnt-report/2018/07/cybercrime-tactics-techniques-q2-2018/ [Accessed 25 November, 2018].

4. Cryptomining. Malware Wikia : site. URL :. http://malware.wikia.com/ wiki/ Cryptomining

5. GandCrab. Malware Wikia : site. URL : http://malware.wikia.com/wiki/ GandCrab [Accessed 25 November, 2018].

УДК 004[681.518]

ПЕТРО СЕРГІЙОВИЧ КЛІМУШИН
кандидат технічних наук, доцент, доцент кафедри інформаційних технологій факультету № 4 Харківського національного університету внутрішніх справ

КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

Комплексний захист інформації ґрунтується на використанні правових, фізичних, організаційних та програмно-апаратних засобів захисту інформації, до яких належить криптографічний захист інформації. Цей вид захисту інформації реалізується шляхом перетворення інформації з використанням ключів на основі математичних методів. Є дві мети використання криптографічних методів – приховування інформації шляхом її шифрування та підтвердження юридичної значимості документів з використанням електронного підпису.

Криптографічні методи вирішують два завдання – забезпечення конфіденційності інформації шляхом позбавлення зловмисника можливості видобути інформацію з каналу зв’язку та забезпечення цілісності інформації шляхом недопущення зміни інформації та внесення в неї неправдивого змісту [1].

Аналіз літературних джерел дає підстави стверджувати, що у процесі використання криптографічних засобів захисту інформації є певні недоліки, які знижують ефективність їх функціонування.

Метою досліджень є надання пропозицій з ефективного використання криптографічних методів і засобів у діяльності органів внутрішніх справ.

Шифрування дозволяє захистити інформацію шляхом її перетворення шифртекст з можливістю подальшого дешифрування. Зашифровувати можна і звичайні тексти, і комп'ютерні файли. Шифрування поділяється на симетричне та асиметричне. В симетричному шифруванні використовується один таємний ключ і для шифрування, і для дешифрування. В асиметричному шифруванні для шифрування використовується відкритий ключ, а для дешифрування – інший, таємний особистий ключ.

Недоліком симетричного шифрування є необхідність передачі ключа особі, що спричиняє загрозу розкриття та дешифрування інформації зловмисниками. Перевагою симетричного шифрування є його більша швидкість, ніж асиметричного, бо під час асиметричного шифрування використовують довші ключі, що збільшує час шифрування.

Симетричні алгоритми шифрування можна розділити на потокові та блочні. Потокові алгоритми шифрування послідовно обробляють текст повідомлення, блочні алгоритми, в свою чергу, працюють з блоками фіксованого розміру.

В сучасних криптосистемах, використовуються комбінації симетричних та асиметричних алгоритмів, для того, аби отримати переваги обох схем. Асиметричні алгоритми використовуються для розповсюдження ключів швидших симетричних алгоритмів.

Для уникнення підміни чи модифікації повідомлення відправник передає отримувачу контрольну суму, яка є унікальною для кожного повідомлення. Для передачі контрольної суми її включають до електронного підпису.

Усунути основні недоліки, властиві як симетричним, так і асиметричним методам криптографічного захисту інформації, дозволяє їх комбіноване використання. У сучасних реальних криптосистемах шифрування даних здійснюється за допомогою «швидких» симетричних блокових алгоритмів, а завданням «повільних» асиметричних алгоритмів стає шифрування ключа сеансу. В цьому випадку зберігаються переваги високої секретності (асиметричні) та швидкості роботи (симетричні).

Електронний підпис дозволяє підтвердити авторство документа та гарантувати цілісність інформації та відсутність спроб її перекручення. Електронний підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа. Підпис повинен залежати від часу, щоб не можна було використати старі повідомлення; цим електронний підпис відрізняється від рукописного підпису.

Електронний підпис дозволяє захистити інформацію від таких злочинних дій: *відмова від авторства* (автор документа відмовляється від авторства); *фальсифікація* (отримувач документа підробляє його); *зміна* (отримувач документа вносить у нього зміни); *маскування* (користувач маскується під іншого користувача) [1].

Документ складається з тексту, електронного підпису та сертифіката користувача, який містить дані користувача, його ідентифікаційне ім'я та відкритий ключ дешифрування для перевірки підпису адресатом документа [2].

Важливою характеристикою методів шифрування є їх криптографічна стійкість, тобто стійкість до дешифрування без ключа, яка визначається як кількість обчислювальних та інших ресурсів для такого дешифрування.

Порядок здійснення криптографічного захисту інформації з обмеженим доступом використовуються криптосистеми і засоби криптографічного захисту допущені до експлуатації Державної службою спеціального зв'язку та захисту інформації України, які мають сертифікат відповідності.

Таким чином, для шифрування з метою передачі інформації в інформаційних мережах доцільно застосовувати асиметричні методи, а для шифрування з метою зберігання інформації – симетричні. Що ж стосується програм для шифрування інформації, то для захисту інформації, яка використовується органами внутрішніх справ, допустимим є використання лише програмних засобів криптографічного захисту інформації, які сертифіковані в Україні.

Список використаних джерел:

1. Зачек О. І. Криптографічний захист інформації у діяльності органів внутрішніх справ. Науковий вісник Львівського державного університету внутрішніх справ. серія юридична. 2014. Вип. 2. С. 91–99.

2. Клімушин П. С. Стратегії та механізми електронного урядування в інформаційному суспільстві. Монографія. Харків. Вид-во ХарРІ НАДУ «Магістр», 2016. 524с.

УДК 343.98

ОЛЕКСАНДР ОЛЕКСАНДРОВИЧ МОЖАЄВ
доктор технічних наук, професор, професор кафедри інформаційних систем факультету №4, Харківського національного університету внутрішніх справ,
МИХАЙЛО ОЛЕКСАНДРОВИЧ МОЖАЄВ
кандидат технічних наук, завідувач лабораторії комп'ютернотехнічних, телекомунікаційних досліджень та досліджень видео-, звукозапису Харківського науково-дослідного інституту судових експертиз ім. Засл. проф. М.С. Бокаріуса
МИХАЙЛО ОЛЕКСАНДРОВИЧ ЛОГВИНЕНКО завідувач сектору комп'ютернотехнічних, телекомунікаційних досліджень та досліджень видео-, звукозапису Харківського науково-дослідного інституту судових експертиз ім. Засл. проф. М.С. Бокаріуса

АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ ЗНИЩЕННЯ ІНФОРМАЦІЇ З МАГНІТНИХ НОСІЇВ ІНФОРМАЦІЇ

Одним із основних завдань, що вирішуються в межах комп'ютерно-технічної експертизи, є встановлення фактів знищення інформації. Органи

досудового розслідування все частіше ставлять на вирішення питання «Чи піддавався досліджуваний накопичувач певним процедурам з метою знищення інформації?». Не зважаючи на наявність зазначеного питання у Науково-методичних рекомендаціях з питань підготовки та призначення судових експертиз та експертних досліджень, затвердженої наказом Міністерства юстиції України від 8 жовтня 1998 року № 53/5 (зі змінами та доповненнями) для його вирішення повністю відсутня методична база і питання вирішується виключно на основі спеціальних знань кожного експерта, що стикається з даною проблемою.

Існує ряд методів знищення інформації, що зберігається на жорсткому диску. Ці методи можна умовно розділити за методом впливу на носій:

• програмні методи - засновані на використанні стандартних команд управління НЖМД;

• апаратні методи - реалізуються за допомогою спеціального обладнання, що впливає на магнітні диски НЖМД. За способом впливу апаратні методи класифікуються на кілька підгруп:

• методи, перебудовують доменну структуру магнітного носія без руйнування його конструкції;

• методи, пов'язані з руйнуванням конструкції носія.

Програмні методи знищення інформації

Всі програмні методи знищення інформації можна за ступенем на-надійності розділити на 3 рівні:

Рівень 0. Найбільш проста і часто застосовуєма форма знищення інформації на НЖМД. Замість повного перезапису жорсткого диска в завантажувальний сектор, основну і резервну таблиці розділів записується послідовність нулів. Тим самим ускладняється доступ до даних, що зберігаються на диску. Самі данні не знищуються. Повний доступ до інформації на НЖМД легко відновлюється за допомогою посекторного читання.

Рівень забезпечує найбільшу швидкість, але не може використовуватися при обробці інформації, витік якої небажана.

Рівень 1. Запис послідовності нулів або одиниць в сектора, які містять інформацію, яку потрібно знищити. Програмний доступ до перезаписаних даних неможливий. Однак існує можливість відновлення інформації після перезапису за рахунок залишкової намагніченості крайових областей дискових доріжок, несе інформацію про попередні записи.

Швидкість знищення інформації значно нижче, ніж в попередньому рівні і визначається швидкістю роботи НЖМД (в основному швидкістю запису).

Рівень 2. Використання декількох циклів перезапису інформації. Зі збільшенням числа циклів перезапису ускладняється завдання відновлення видалених даних. Це обумовлюється природним дрейфом друкарській головки НЖМД під час кожного наступного циклу. Імовірність перезапису

крайових областей доріжок зростає. Отже, різко підвищується складність процесу відновлення знищених даних.

Повної гарантії незворотного руйнування інформації немає і в цьому випадку, оскільки програмно неможливо управляти траєкторією руху блоку головок НЖМД і процесом перемагнічування бітових інтервалів. Крім того, знищення інформації ускладнено через складність оцінки факторів, що впливають на точність позиціонування головок.

Недоліком методів цього рівня є низька швидкість знищення інформації.

Апаратні методи знищення інформації

Підвищену надійність знищення інформації, що зберігається на жорсткому диску, забезпечують апаратні методи. Недоліком цих методів є повне або часткове руйнування накопичувача.

Перебудова доменної структури магнітного носія

Оптимальним підходом для забезпечення надійного знищення інформації без фізичного знищення носія є використання методів, що призводять до перебудови структури магнітного матеріалу робочих поверхонь носія. Для цього необхідно усунути неоднорідності вектора намагніченості на доріжках НЖМД. Зміна структури намагніченості магнітного шару може бути виконано кількома принципово різними способами:

• шляхом швидкого нагрівання матеріалу робочого шару носія до точки втрати намагніченість носія (точки Кюрі);

• шляхом розмагнічування робочих поверхонь носія;

• шляхом намагнічування робочих поверхонь носія до максимально можливих значень намагніченості (насичення);

• комбінований. Нагрівання і намагнічування, або нагрівання і розмагнічування.

Руйнування конструкції носія

Методи цієї групи застосовують, коли необхідна гарантія знищення інформації. Вони підрозділяються на:

• механічні;

• хімічні - руйнування робочого шару або основи носія за допомогою хімічно агресивних середовищ;

• термічні - метод полягає в нагріванні носія до температури плавлення в спеціальних печах. Гарантія знищення інформації може бути отримана при розігріві носія до температури 800-1000'С;

• радіаційні - руйнування носія за допомогою використання іонізуючих випромінювань.

Таким чином, були розглянуті існуючи методи знищення інформації з магнітних носіїв інформації.

УДК [351.74:004](091)(47
МИХАЙЛО ЮРІЙОВИЧ БУРДІН
доктор юридичних наук, професор,
проректор Харківського національного університету внутрішніх справ,
ВОЛОДИМИР ПЕТРОВИЧ КУБРАК
ЮРІЙ ПЕТРОВИЧ ГОРЕЛОВ
кандидат технічних наук, доцент, доцент кафедри інформаційних технологій
факультету № 4 Харківського національного університету внутрішніх справ

ІСТОРІЯ ПІДГОТОВКИ ФАХІВЦІВ ДЛЯ ІНФОРМАЦІЙНО-АНАЛІТИЧНИХ ПІДРОЗДІЛІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ У ХНУВС

Перший набір курсантів на єдиний в Україні факультет з підготовки фахівців для інформаційно-аналітичних служб МВС України інституту внутрішніх справ м. Харкова був здійснений у 1993 році за спеціальністю «Правознавство» з поглибленим вивченням дисциплін комп'ютерного циклу і терміном навчання 5 років. Першим начальником факультету був призначений підполковник міліції Погуляєв Сергій Юрійович. В цьому ж році було створено дві профільні кафедри цього напряму – кафедра інформатики і спеціальної техніки (перший начальник кафедри – підполковник міліції, кандидат технічних наук, доцент Кухарьонок Михайло Андрійович) та кафедра прикладної математики (перший начальник кафедри – підполковник міліції, доктор фізико-математичних наук, професор Яковлев Сергій Всеволодович). В подальшому з 1994 року було започатковано набір на комп'ютерні спеціальності, а в 1996 році була створена випускаюча кафедра інформаційних технологій в діяльності ОВС (перший начальник кафедри – майор міліції, кандидат технічних наук, доцент Струков Володимир Михайлович), а факультет з 1995 року очолив підполковник міліції, доктор фізико-математичних наук, професор Яковлев Сергій Всеволодович.

В березні 2006 року згідно наказу МВС України № 220 від 3.03.2006 р. в складі Харківського національного університету внутрішніх справ був створений навчально-науковий інститут права, економіки та соціології ХНУВС, в складі якого серед інших були створені три кафедри технічного профілю - кафедра інформаційних систем і технологій (З 2006 року по 2010 завідувачами кафедри були кандидат технічних наук, доцент Лановий О.Ф. (2006-2007) та кандидат технічних наук, доцент Горелов Ю.П. (2007-2010)), кафедра інформатики та прикладної математики (завідувач – кандидат технічних наук, доцент Шеховцов Сергій Борисович) та кафедра захисту інформації (завідувач – кандидат технічних наук, доцент Пєвнєв Володимир Якович). Перші дві кафедри готували бакалаврів за напрямом 0501 - Комп'ютерні науки, спеціалістів та магістрів за спеціальністю 050101 –

Інвормаційно-управляючі системи і технології. Кафедра захисту інформації готувала бакалаврів за напрямом 170102 – Системи технічного захисту інформації та спеціалістів за спеціальністю 17010201 - Системи технічного захисту інформації, автоматизація її обробки.

У 2010 році навчально-науковий інститут права, економіки та соціології був реорганізований у навчально-науковий інститут права та масових комунікацій. Під час реорганізації кафедра інформаційних систем і технологій та кафедра інформатики та прикладної математики були об'єднані в кафедру математичного моделювання та інформаційних технологій. Завідувачем кафедри був призначений Герасін Сергій Миколайович, доктор технічних наук з 2006 року за спеціальністю 01.05.02 «Математичне моделювання та обчислювальні методи». професор по кафедрі вищої математики ХНУРЕ з 2008 року.

З початку 2013 року кафедру очолював кандидат технічних наук, доцент Горєлов Юрій Петрович.

Кафедра захисту інформації у 2010 році була реорганізована в кафедру інформаційних комунікацій, захисту інформації та документознавства (завідувач – кандидат технічних наук, доцент Пєвнєв Володимир Якович). З квітня 2011 року кафедру очолював кандидат технічних наук, доцент Струков Володимир Михайлович.

У липні 2013 року кафедру математичного моделювання та інформаційних технологій та кафедру інформаційних комунікацій, захисту інформації та документознаства об'єднано в кафедру інформаційних технологій та захисту інформації. Завідувачем створеної кафедри призначено кандидата технічних наук, доцента Струкова Володимира Михайловича.

Кафедра здійснювала навчання студентів за напрямом 6.170102 „Системи технічного захисту інформації" та спеціальністю 8.080401 „Інформаційні управляючі системи та технології". Вона також забезпечувала викладання дисциплін в галузях інформаційних технологій та інформаційної безпеки на всіх контрактних спеціальностях ХНУВС.

З 2016 року на факультеті № 4 започатковано підготовку фахівців за спеціальністю «Кібербезпека».

В лютому 2017 року шляхом об'єднання кафедри інформаційної безпеки факультету № 4 з кафедрою інформаційних технологій і захисту інформації факультету № 6 була створена кафедра інформаційних технологій факультету № 4. Кафедра є структурним підрозділом університету, що проводить навчально-виховну, методичну, а також науково-дослідну діяльність із метою підготовки курсантів, слухачів і студентів в галузі інформаційних технологій та інформаційної безпеки.

УДК 004.89

ЮРІЙ ВАЛЕРІЙОВИЧ ГНУСОВ,
кандидат технічних наук, доцент, завідувач кафедри кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ
ЮРІЙ МИКОЛАЙОВИЧ ОНИЩЕНКО,
кандидат наук з державного управління, доцент, доцент кафедри кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

КОНЦЕПТУАЛЬНІ ПІДХОДИ ДО ОРГАНІЗАЦІЇ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ ДІЯЛЬНОСТІ ПОЛІЦІЇ

Зростання масштабів, складності та динамізму правоохоронної практики вимагають на сучасному етапі принципового вдосконалення діючої системи інформаційно-аналітичного забезпечення. Її основне завдання полягає в зборі та переробці інформації, необхідної для прийняття обґрунтованих управлінських рішень на всіх рівнях організації Національної поліції України. У той же час, мова йде саме про систему інформаційно-аналітичного забезпечення, що складається з ряду взаємопов'язаних елементів (структура системи):

- інформації, необхідної для виконання однієї або кількох функцій управління підрозділами поліції;
- персоналу, що забезпечує функціонування інформаційної системи;
- необхідних технічних засобів;
- методів і процедур збору та переробки інформації;
- методів і процедур аналізу інформації.

Мова йде про співвідношення оперативних, тактичних і стратегічних управлінських рішень, а, отже, про специфіку інформаційно-аналітичного процесу їх вироблення.

Зокрема, необхідною умовою організації аналізу злочинності в регіоні, районі є інформаційно-аналітичне забезпечення оперативних завдань поліції, що має на увазі прогнозування, аналіз та планування конкретних слідчих (розшукових) та негласних слідчих (розшукових) дій, оперативно-розшукових та захисних заходів. Так, для оперативних підрозділів – це добірки оперативних матеріалів, справи оперативного обліку, матеріали вивчення кандидатів на негласне співробітництво тощо; для слідчих підрозділів – матеріали кримінальних проваджень тощо.

До форм інформаційно-аналітичної діяльності належать: плани оперативно-розшукових заходів по добірками оперативних матеріалів, справах оперативного обліку, плани активізації фігурантів при проведенні оперативно-технічних і пошукових заходів, схеми зв'язків, результати ОРД, легалізовані оперативними підрозділами, рапорти на реєстрацію матеріалів, інші оперативно-службові документи.

Для слідчих підрозділів характерно складання постанов про порушення кримінальних проваджень, постанов про закриття кримінальних проваджень,

планів слідчих (розшукових) заходів, постанов про притягнення до кримінальної відповідальності в якості підозрюваного (обвинуваченого) тощо.

Інформаційно-аналітичне забезпечення тактичних завдань оперативно-службової діяльності поліції передбачає прогнозування, аналіз та планування заходів, об'єднаних за родовою ознакою. На нашу думку, це найбільш істотний аспект, який вказує на особливості саме тактичного управління. До таких заходів слід віднести організацію роботи по лініях (напрямках, ділянках, об'єктах) оперативного обслуговування, розробку відповідними фахівцями методичних рекомендацій з найважливіших питань оперативно-службової діяльності підрозділів поліції.

Суб'єктами інформаційно-аналітичної діяльності виступають: аналітичні, оперативні та слідчі підрозділи. Особливістю організації інформаційно-аналітичної діяльності є те, що аналітичний підрозділ обслуговує, перш за все, потреби оперативних підрозділів, як ініціаторів проведення практично всіх перевірок. При грамотній організації роботи, такі ланки, як оперативний підрозділ – аналітичний підрозділ – інші підрозділи поліції автоматично (кожне на своєму етапі) вступають в загальний процес оперативно-службової діяльності, метою якого є комплексна реалізація поставлених завдань в єдиному оперативному ключі.

Інформаційно-аналітичне забезпечення стратегічних завдань оперативно-службової діяльності поліції полягає в зборі оперативно-значущої інформації в масштабах території оперативного обслуговування, стратегічному аналізі та прогнозуванні розвитку криміногенної обстановки, складанні переліку загроз безпеці регіону, вироблення спільних рекомендацій для керівництва територіальних органів.

Формами інформаційно-аналітичної діяльності є: концепція розвитку поліції, концепції розвитку окремих видів оперативно-службової діяльності, довідки про оперативну обстановку і результати діяльності територіальних органів, інші аналітичні документи, що зачіпають питання організації оперативно-розшукової та слідчої діяльності регіонального підрозділу в цілому на термін від одного року і більше.

Таким чином, всі учасники інформаційно-аналітичної діяльності в переважній більшості випадків користуються фактичними результатами оперативно-службової діяльності.

УДК 004:35:321.7:001.89
ДМИТРО ЮРІЙОВИЧ ХЛАПОНІН
здобувач Інституту підготовки кадрів Державної служби зайнятості України

МЕХАНІЗМИ ДЕРЖАВНОГО УПРАВЛІННЯ ПРОЦЕСАМИ РЕЄСТРАЦІЇ ФІЗИЧНИХ ОСІБ ТА ЇХ ДОКУМЕНТУВАННЯ

Кіберфізичні системи (КФС) - це інтелектуальні системи, що включають інженерно-взаємодіючі мережі фізичних та обчислювальних компонентів [1, с. 5]. Об'єднання цих компонентів у межах єдиної системи дає змогу отримувати якісно нові результати, які можна використовувати для створення широкого спектра принципово нових наукових, технічних та сервісних засобів. Створення та функціонування КФС потребують законодавчого врегулювання та впровадження механізмів державного управління кіберфізичними системами. Тому очевидна необхідність комплексного теоретичного обґрунтування, впровадження правового забезпечення КФС, напрацювання науково обґрунтованих пропозицій з цього питання та рекомендацій, спрямованих на впровадження механізмів державного управління створенням та функціонуванням кіберфізичних систем, подальше вдосконалення правозастосовної практики у цій сфері [2, с. 6].

Завдяки впровадженню КФС можуть бути автоматизовані наступні технологічні процеси в Україні:

- діяльність по виконанню державних функцій та послуг у сфері міграції;
- оформлення і видача громадянам України документів, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус;
- аналіз міграційної ситуації в Україні, проблем питань пов'язаних із біженцями та іншими категоріями мігрантів,
- ідентифікація громадян України, які втратили документи, що посвідчують особу.

АРМ користувача є інтегрованою складовою сервіс-орієнтованої архітектури інформаційної системи, яка призначена для автоматизації діяльності у сфері реєстрації фізичних осіб та їх документування, включаючи оформлення паспорту громадянина України для виїзду за кордон з безконтактним електронним носієм.

Для оформлення документів СПЗ «Паспорт» повинне функціонувати на автоматизованому робочому місці (АРМ) з комплектом обладнання взяття біометричних даних.

До складу АРМ входять:

А) засоби взяття біометричних даних фізичних осіб:

- фотоапарат;
- біометричний сканер відбитків пальців рук та підпису;

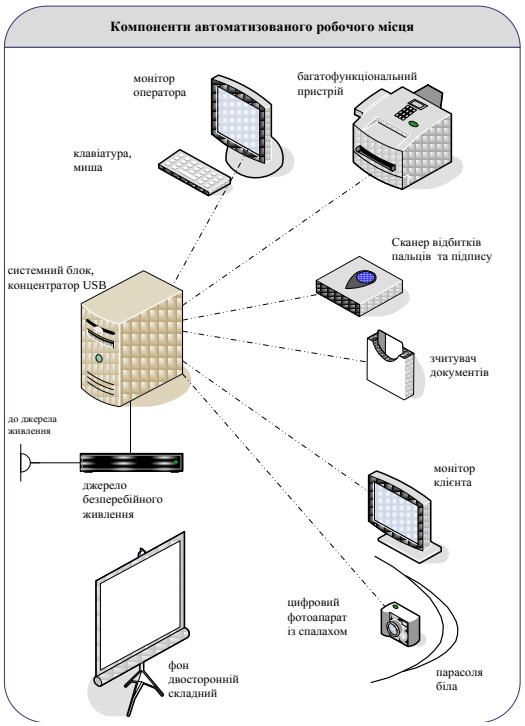
Б) пристрій зчитування інформації (e-READER) з машинозчитуваної зони документу (MRZ) та безконтактного електронного носія.

В) багатофункціональний пристрій (принтер + сканер).

Інформація, що містить відомості про особу (персональні дані), повинна захищатись у відповідності до вимог Закону України «Про захист персональних даних». Згідно з статтею 8 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах»: *«…Державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинна оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю.*

Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, встановленому законодавством…» [3, с. 4].

У відповідності до п.16 Постанови Кабінету міністрів України № 373 від 29.03.2006 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах»: «…Для забезпечення захисту інформації в системі створюється комплексна система захисту інформації, яка призначається для захисту інформації від несанкціонованих дій з інформацією та спеціального впливу на засоби обробки інформації, який здійснюється шляхом формування фізичних полів і сигналів та може призвести до порушення її цілісності та несанкціонованого блокування…». Проблема полягає в підтримці балансу між збереженням конфіденційності та захистом персональних даних - і доступністю даних для надання більш якісного обслуговування. Оскільки КФС керують значними обсягами даних, що включають таку конфіденційну інформацію, як здоров'я, стать, віросповідання і багато інших персональних відомостей, виникають серйозні проблеми захисту персональних даних. Для КФС необхідні політики забезпечення конфіденційності, тому потрібен інструмент знеособлення даних, що дозволяє видаляти персональну інформацію перед обробкою даних системою [4, с. 7].



Таким чином, в зв’язку з бурхливим розвитком КФС та неминучістю такого розвитку постає необхідність приведення національного законодавства України до міжнародних стандартів, покладення на відповідні державні органи чітких повноважень в сфері КФС, ліквідації потенційних інноваційних бар'єрів, встановлених існуючими нормами, недостатніми для функціонування КФС, удосконалення методів та інструментів для сертифікації КФС.

Список використаних джерел

1. Framework for Cyber-Physical Systems Release 1.0 May 2016 Cyber Physical Systems Public Working Group, www.nist.gov.

2. Рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України".

3. Закон України «Про основні засади забезпечення кібербезпеки України" (Відомості Верховної Ради (ВВР), 2017, № 45, ст.403).

4. Кібербезпека в інформаційному суспільстві, Інформаційно-аналітичний дайджест, № 12 (грудень), Київ – 2017.

УДК 351

ТЕТЯНА ПЕТРІВНА КОЛІСНИК
кандидат педагогічних наук, доцент, доцент кафедри інформаційних технологій факультету № 4 Харківського національного університету внутрішніх справ

ВИДИ ДЖЕРЕЛ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ПОШУКУ

Департамент інформаційно-аналітичної підтримки Національної поліції України є структурним підрозділом центрального органу управління поліції, який здійснює заходи, передбачені законодавством України, що спрямовані на інформаційно-аналітичне та інформаційно-пошукове забезпечення та захист персональних даних при їх обробленні в структурних підрозділах центрального органу управління поліції, міжрегіональних територіальних органах Національної поліції України, територіальних органах поліції в Автономній Республіці Крим та м. Севастополі, областях, м. Києві, у тому числі їх територіальних (відокремлених) підрозділах [1].

Завдання інформаційного пошуку стосується пошуку інформації в документах, пошуку самих документів, вилучення метаданих з документів, пошуку тексту, фото-, відеоматеріалів, аналізу інформації з гіпертекстових баз даних. Залежно від наявного обсягу первинних даних необхідно розрізняти два напрями пошуку.

Інформаційний пошук – варіант пошуку інформації за наявності анкетних даних, достатніх для ідентифікації особи та перевірки за відомчими обліками, базами даних, відкритими джерелами інформації.

Інформаційно-аналітичний пошук – варіант пошуку інформації за наявності мінімальних даних (електронна адреса, фото, номер телефону тощо), які прямо не можуть вказати на особу, але за допомогою використання джерел інформаційно-аналітичного пошуку можна встановити анкетні дані особи [2, с.4].

Серед основних джерел пошуку інформації про фізичних осіб можна виділити такі: бази даних правоохоронних органів та обліки даних (пошукові системи відкритого типу з інформацією про осіб, що раніше потрапляли в поле зору правоохоронних органів); соціальні мережі; адресні бази; мета пошукові системи; реєстри про власність, розміри доходів, займані посади; сайти з інформацією компрометуючого характеру.

Джерела інформаційно-аналітичного пошуку за характером отримуваної інформації можна поділити на:

1. *Відомчі бази* – бази даних правоохоронних органів та обліки з інформацією про осіб, що раніше потрапляли в поле зору правоохоронних органів.

2. *Державні реєстри* – автоматизовані системи обліку інформації про осіб, майно, документи, які створюються та ведуться державою з метою реалізації своїх функцій. Поділяються на два види – *відкриті та закриті:*

а) відкриті містять інформацію, отриману з джерел, доступ до яких для більшості громадян не обмежений законодавчими або іншими нормами; ця інформація характеризується систематичною публікацією в офісних друкованих виданнях (бюлетенях, збірниках), поширенням засобами масової інформації, безпосереднім наданням державними органами громадянам та юридичним особам. До них належать:

- **обліки даних** (пошукові системи відкритого типу з інформацією про осіб, що раніше потрапляли в поле зору правоохоронних органів): http://www.reyestr.court.gov.ua

Якщо відомий факт притягнення особи до відповідальності в порядку адміністративного, господарського, цивільного чи кримінального судочинства, можливе використання Єдиного державного реєстру судових рішень, у якому розміщено судові рішення (висновки, рішення, ухвали, постанови, судові накази) з текстом та деталями самого рішення;
https://myrotvorets.center

Якщо відомо, що особа могла бути причетна до вчинення злочинів проти основ національної безпеки України, можливе застосування пошуку через сайт «Миротворець» неурядової організації, що займається дослідження ознак злочинів проти основ національної безпеки України, миру, безпеки людства та міжнародного правопорядку. На цьому сайті міститься інформація про осіб зазначеної категорії з розміщенням фото та зазначенням сторінок у соціальних мережах, особистих даних;
https://opendatabot.com

Відомості щодо фізичної особи, яка займається підприємницькою діяльністю, чи юридичної особи можна з’ясувати за допомогою «opendatabot» - сервісу моніторингу реєстраційних даних українських компаній та судового реєстру для захисту від рейдерських захоплень і контролю контрагентів. Тут зібрано інформацію з відкритих державних реєстрів та інших джерел, яку можна миттєво отримати як повідомлення на Telegram, Facebook, Messenger, Skype або Viber;
https://Youcontrol.com.ua

Ресурс формує повне досьє на кожну компанію України. Тут відображено відомості про юридичних осіб, їх статус, контактну інформацію, юридичну адресу, судові рішення, пов’язані з компаніями, та інші дані, які перебувають у відкритому доступі;

- **адресні бази** - це відкриті адресні бази, інформацію з яких можна отримати за наявності мінімуму даних (прізвище чи адреса).

http://www.nomer.org/allukraina - Вся Україна - жителі;

- **реєстри про власність, розміри доходів, займані посади;**

б) закриті містять інформацію, що характеризується обмеженням кола осіб, що мають доступ до неї, відповідальністю за достовірність відомостей, що повідомляються, та відповідальністю особи, яка її використовує та поширює.

3. *Соціальні мережі*: - веб-сайти, які дозволяють користувачам створювати публічну або напівпублічну анкету, складати список користувачів, з якими вони мають зв'язок, та переглядати власний список зв’язків і списки інших користувачів (Facebook, Instagram, Odnoklassniki, Ukr.net, Vk.com, Twitter тощо).

4. *Засоби масової інформації* – система установ та закладів, створених з метою публічного, оперативного поширення інформації про події та явища у світі, країні чи регіоні серед необмеженого кола осіб і суб’єктів та зорієнтованих на виконання певних суспільних завдань.

Сайти з інформацією компрометуючого характеру: http://compromat.ua, http://dosye.co.ua, http://strelaua.com, http://antikor.com.ua, https://ord-ua.

Метапошукові системи – це пошуковий інструмент, який надсилає запит одночасно декільком пошуковим системам, каталогам та, інколи, у так звану невидиму (приховану) павутину – зібрання он-лайнової інформації, не проіндексованої традиційними пошуковими системами. На відміну від окремих пошукових систем і директорій, мета пошукові системи не мають власних баз даних і не реєструють URL-адреси сайтів. Метапошуком варто користуватися якщо документів за запитом мало. (Yippy, Dogpile, Nigma, Search, Weblib) [3, с.203].

Список бібліографічних посилань

1. Наказ НПУ від 11.10.2017 № 1060 «Про затвердження Положення про Департамент інформаційно-аналітичної підтримки Національної поліції України».

2. Методичні рекомендації щодо здійснення інформаційно-аналітичного пошуку / О.С. Клінг, Т.В. Миронова, Я.В. Серб, Р.Г. Аноколова // Національна поліція України. Ситуаційний Центр. – Киев, 2017. – 38 с.

3. Прокопов С.О. Використання пошуку інформації з відкритих джерел мережі Інтернет у навчальному процесі Дніпропетровського державного університету внутрішніх справ / С.О. Прокопов // Проблеми застосування інформаційних технологій правоохоронними структурами України та ВНЗ зі специфічними умовами навчання. : збірник наукових статей за матеріалами доповідей учасників міжнародної науково-практичної конференції (22 грудня 2017 р., м. Львів). – Львівський державний університет внутрішніх справ, 2017. – С. 202-204.

УДК 378; 371
МУРАТ ВСЕВОЛОДОВИЧ МАЛЯРОВ
кандидат технічних наук, доцент, доцент кафедри автоматичних систем безпеки та інформаційних технологій Національного університету цивільного захисту України
ВАЛЕРІЙ ВОЛОДИМИРОВИЧ ХРИСТИЧ
кандидат технічних наук, доцент, заступник начальника кафедри автоматичних систем безпеки та інформаційних технологій Національного університету цивільного захисту України

ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У СТВОРЕННІ ІГРОВИХ ФОРМ В ПІДГОТОВЦІ ФАХІВЦІВ

Сучасні умови висувають підвищені вимоги до системи якості підготовки фахівців, зокрема, НПУ. Сьогодні випускник ВНЗ стає більш активним суб'єктом на ринку праці, вільно розпоряджається своїм головним капіталом - професією, спеціальністю, кваліфікацією. Системні зміни, що відбуваються, також вплинули і на підготовку фахівців сфери МВС.

Згідно з висновками фахівців екстремальної та кризової психології ефективному вивченню спеціалізованих фахових предметів найбільш оптимально в інтелектуальному плані підготовлена лише половина майбутніх випускників спеціалізованих ВНЗ. Існуючі в сьогоденній практиці вивчення спеціалізованих фахових предметів протиріччя між підвищенням теоретичного рівня вивчення предмета на початковому його етапі та недостатньою сформованістю навичок логічного мислення породжує своєрідний психологічний бар'єр, який призводить до різкого зниження інтересу до вивчення предмету.

В теперішній час все частіше наголошується на те, що причина незадовільної якості загальноосвітньої підготовки слухачів, їх слабких знань міститься в тому, що класичні заняття, як форма навчання, застаріли та не завжди ефективно стимулюють пізнавальну діяльність здобувачів освіти і не відкривають простору для методичної творчості. У сучасних умовах завдання підготовки грамотних і висококваліфікованих фахівців, як-то, для НПУ, ДСНС, НГУ тощо, може бути вирішено шляхом творчого засвоєння знань і методів діяльності, які формують творче мислення здобувачів освіти.

Питання про формування інноваційних знань, умінь і відносин майбутніх фахівців, їх креативності та самостійності у професійній діяльності ефективно вирішується при впровадженні в освітній процес вишу активних методів навчання, серед яких все більш значущим і продуктивним педагогічним засобом стають ігрові технології. Заняття з використанням ігрових технологій викликають жвавий інтерес у слухачів, який в свою чергу, стимулює пізнання, мотивує процес навчання. Навчальні дидактичні ігри розвивають і закріплюють у студентів навички самостійної роботи, вміння професійно мислити, вирішувати завдання і вести управління колективом,

приймати рішення і організовувати їх виконання. В ході гри виробляються саме професійні вміння та навички:

збору і аналізу інформації, необхідної для прийняття рішень, відповідно до змодельованої ситуації;

прийняття рішень в умовах неповної чи недостатньо достовірної інформації, оцінка ефективності прийнятих рішень;

аналізу певного виду завдань;

встановлення зв'язків між різними сферами майбутньої професійної діяльності;

роботи в колективі, вироблення колегіальних рішень з використанням прийомів групового рішення;

абстрактного та образного мислення, як основи ефективного творчого використання системного підходу до дослідження процесів і явищ.

Ігрове навчання використовувалося при підготовці здобувачів освіти ДСНС освітньо-кваліфікаційного рівня "магістр" у рамках вивчення технічного курсу за напрямом "автоматичні системи безпеки". Гра проводилась в комп'ютерному класі зі спеціально створеною програмою. Під час гри перевірялися не тільки швидкість реакції, пам'ять та увага, а й спеціальні знання з предметної області. Таким чином, заняття, що проводяться у вигляді гри, вимагають від кожного учасника об'єктивної оцінки своїх можливостей; сприяють правильному сприйняттю критики товаришів і невимушеному спілкуванню, вмінню співвідносити і порівнювати власне судження з думкою однокурсників, формувати професійний інтерес, вміння співвідносити ситуацію і швидко приймати найбільш правильне рішення. В процесі проведення ігор виникають проблемні ситуації і дискусії, які важко створюються на звичайному практичному занятті. Проведення нестандартних занять викликає жвавий інтерес в учнів, а інтерес є стимулом пізнання і мотивує процес навчання.

Ігрові технології можна використовувати як при проведенні занять, так і під час самостійної роботи. Безумовно, створення будь-якої гри буде залежати від конкретних умов навчання, а самі ігри можна використовувати як на протязі вивчення всього предмету, так і під час модульного або підсумкового контролю.

Список використаних джерел

1. Ханнанова-Фахрутдинова Л.Р. Дидактическая игра как средство организации подготовки компетентных специалистов для легкой промышленности / Л.Р. Ханнанова-Фахрутдинова, О.Ю. Хацринова // Вестник Казан. технол. Ун-та, 2010, № 12. – С. 346-350.

2. Мачинська Н.І. Впровадження ігрових технологій навчання у практику підготовки майбутніх магістрів [електронний ресурс] Режим доступу: http://lib.chdu.edu.ua/pdf/naukpraci/pedagogika/2011/158-146-3.pdf.

УДК 372.862
ВОЛОДИМИР ВОЛОДИМИРОВИЧ ТУЛУПОВ
кандидат технічних наук, доцент,
доцент кафедри інформаційних технологій
факультету № 4 Харківського національного
університету внутрішніх справ
ВАЛЕРІЙ МИКОЛАЙОВИЧ ПЕРЕСІЧАНСЬКИЙ
старший викладач кафедри інформаційних технологій факультету № 4
Харківського національного університету внутрішніх справ

РОЗРОБКИ ТА ВПРОВАДЖЕННЯ КОМПОНЕНТІВ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ОСВІТНЬОМУ ПРОЦЕСІ КАФЕДРАМИ ЗІ СПЕЦИФІЧНИМИ УМОВАМИ НАВЧАННЯ

Розробка та впровадження компонентів інформаційних технологій для підготовки фахівців з організації захисту інформації має суттєву прикладну компоненту наближення до проблематики діяльності підрозділів технічного захисту інформації правоохоронних органів. Комп'ютеризація та тренажерізація відносяться до числа найбільш наукомістких областей, що вимагають величезних витрат інтелектуальної праці, у тому числі праці методистів вищої кваліфікації.

Щоб представити масштаб проблем, досить звернути увагу на такі фактори.

По-перше, найбільш ефективна комплексна комп'ютеризація та тренажерізація професійної підготовки фахівців, що забезпечують усі стадії життєвого циклу виробу: проектування, розробку, випробування, виробництво, експлуатацію, технічне обслуговування, ремонт та успішного виконання учбового завдання [1, с. 237].

По-друге, розробка однієї години високоефективної навчальної комп'ютерної програми, як показує вже наявний досвід, вимагає витрат багатьох людино-годин праці кваліфікованих програмістів і методистів. При цьому контроль якості навчаючих програм та ефективності тренажерної підготовки є справою складною, що потребує спеціальних знань, тестів, участі експертів тощо. Без такого контролю та сертифікації можливі негативні результати навчання, виникнення помилкових навичок, втрати природного інтелекту у особи, що навчається та ін. Також до цього варто додати констатацію неухильного зросту вартості апаратних і програмних засобів як існуючих тренажерів так і інших навчаючих інтерактивних систем.

По-третє, високий темп розвитку інформаційних технологій зумовлює:

– оновлення засобів матеріально-технічного забезпечення навчального процесу новими зразками техніки та інформаційними технологіями;

– оновлення кадрового потенціалу кафедр зі специфічними умовами навчання та взаємопроникнення інформаційних технологій та спеціальних знань в суміжні дисципліни, що викладаються;

– впровадження нових методик і прийомів навчання, комп’ютеризація та інформатизація навчального процесу;

– тісний зв'язок з передовими науково-технічними розробками в сфері інформаційних технологій та спеціальної техніки [1, с. 238].

Метою даної доповіді є виділення кола існуючих проблем щодо програмно-технічного забезпечення нормативних дисциплін кафедр зі специфічними умовами навчання та шляхи їх подальшої реалізації на прикладі створення комп'ютерних навчаючих систем (комп'ютерних тренажерів) та впровадження їх у навчальний процес.

На теперішній часу у освітній сфері пропонуються різні тренажерні комплекси (комп'ютерні тренажери) у тому числі із організації захисту інформації наприклад:

– навчаючий тренажерний комплекс «Зоря», що призначений для підготовки фахівців в галузі атестації об'єктів;

– програмно-апаратний комплекс «Салют», що призначений для пошуку та локалізації відеокамер та акустичних розвідувальних засобів, включаючи тренажер для підготовки операторів;

– навчаючий тренажерний комплекс «Спектр», що призначений для підготовки фахівців в галузі пошуку та виявлення радіозакладних пристроїв) ;

– автономний імітатор радіозавад «Кобра», що призначений для імітації постановки завад радіоелектронним засобам різного призначення та типу з метою навчання операторів розв'язанню задач в умовах дії навмисних завад, а також відпрацювання дій груп пошуку та знищення передавачів завад, що були занесені та/або встановлені [2].

Наприклад, вищезазначені тренажерні комплекси, а також існуючи розробки кафедр зі специфічними умовами навчання, дозволять у деякій мірі замінити тренування на штатних існуючих або відсутніх на таких кафедрах або в практичних підрозділах приладів – засобами сучасних інформаційних технологій, шляхом виконання учбово-тренувальних задач за допомогою інтерактивного середовища на персональному комп'ютері.

Впровадження нових методик навчання здійснюється також в системі відомчої освіти, зокрема в Харківському національному університеті внутрішніх справ, де здійснюється підготовка фахівців за спеціальністю 125 – «Кібербезпека».

Розв'язання деяких вищезазначених проблем знайшли своє відображення у розробках кафедр «Інформаційних технологій» та «Кібербезпеки» факультету № 4, наприклад: комп'ютерний тренажер «Селективний мікровольтметр та вимірювач напруги завад SMV 8.5» призначений для отримання курсантами та студентами первинних практичних навичок роботи з селективним мікровольтметром та вимірювачем напруги завад SMV 8.5.

Тренажер являє собою спрощений інтерактивний аналог (сімулятор) пристрою SMV 8.5 та має наступні можливості:

– ознайомлення користувача з призначенням пристрою;

– ознайомлення з технічними характеристиками SMV 8.5;

– ознайомлення з комплектацією пристрою;

– ознайомлення з органами управління пристроєм;

– демонстрація використання пристрою при виконанні учбово-тренувальних задач;

– безпосереднє виконання учбово-тренувальних задач для оволодіння навичками роботи з пристроєм;

– тестування користувача.

Також для забезпечення проведення лабораторних робіт з дисциплін: «Методи та засоби захисту інформації», «Метрологія та вимірювання», «Електроніка та схемотехніка» також було розроблено комп'ютерні тренажери а саме: «Виміри за допомогою селективного мікровольтметру SMV 11», «Виміри за допомогою селективного нановольтметру Unipan-233» та «Вимірювач шуму та вібрацій ВШВ-003-М2» з використанням мультимедійної платформи Adobe Flash та інших технологій. У рамках дипломного проектування розробляються комп'ютерні тренажери для інших пристроїв з подальшим впровадженням їх у навчальний процес.

Висновки. Впровадження таких розробок у навчальний процес дозволить у деякій мірі замінити традиційний науковий інструментарій засобами сучасних інформаційних технологій, шляхом виконання учбово-тренувальних задач на комп'ютерному тренажері, у зв'язку з обмеженістю таких приладів як на кафедрах зі специфічними умовами навчання, так і в практичних правоохоронних підрозділах.

Література:

1. Тулупов, В.В. Актуальні аспекти побудови комп'ютерних тренажерів для професійної підготовки кадрів органів внутрішніх справ [Текст] / В.В. Тулупов, О.М. Рвачов // Матеріали науково-практичної конференції (Київ, 25 листоп. 2011 р.) «Спеціальна техніка у правоохоронній діяльності». – К.: НАВС, 2012. – С. 236-239.

2. «НЕЛК» Научно-производственный центр [Електронний ресурс]. – Режим доступу: http://www.pemi.ru

УДК 004.492.2

ІГОР ВОЛОДИМИРОВИЧ КОБЗЕВ
кандидат технічних наук, доцент, доцент кафедри природознавчих наук Харківського національного університету радіоелектроніки
ВІКТОРІЯ АНАТОЛІЇВНА ЛУК'ЯНОВА
кандидат педагогічних наук, доцент, завідувач кафедри природознавчих наук Харківського національного університету радіоелектроніки

ЦИФРОВА ЕКОНОМІКА ТА КІБЕРБЕЗПЕКА

Поняття «digital economy» належить бізнес-аналітику Дону Тапскоту. Ще наприкінці XX століття він у доступній формі намагався пояснити підприємцям, як пов'язані кардинальні зміни в світі технологій зі змінами в бізнесі. Цифрова економіка — це економічна діяльність, яка, на відміну від

традиційної економіки, визначається мережевою свідомістю (networked intelligence) та залежністю від віртуальних технологій [2].

У середині січня 2018 року Кабінет Міністрів України ухвалив «цифрову стратегію» на найближчі роки. Відтак український медійний простір сколихнули матеріали про цифрову економіку, електронний бізнес та перспективи впровадження віртуальних технологій [3].

У цій стратегії наступні загрози і виклики:

— проблема забезпечення прав людини у цифровому світі, у тому числі при ідентифікації, збереженні цифрових даних користувача, а також проблема забезпечення довіри громадян до цифрового середовища;

— загрози особи, бізнесу і державі, пов'язані з тенденціями до побудови складних ієрархічних інформаційно-телекомунікаційних систем, що широко використовують віртуалізацію, видалені (хмарні) сховища даних, а також різнорідні технології зв'язку і пристрої;

— ріст масштабів комп'ютерної злочинності, у тому числі міжнародної;

— відставання від провідних іноземних держав в розвитку конкурентоздатних інформаційних технологій;

— недостатня ефективність наукових досліджень, пов'язаних із створенням перспективних інформаційних технологій, низький рівень впровадження вітчизняних розробок, а також недостатній рівень кадрового забезпечення в області інформаційної безпеки.

Серед першочергових завдань впровадження цифрової економіки вимагають негайного рішення наступні завдання:

— надання легітимності використання криптовалют як форми розрахунків в деяких сферах економіки держави. У ВР України зареєстровано п’ять законопроектів, які передбачають визначення правового статусу крипти у країні [1]. Актуальність цього завдання пояснюється тим, що в умовах відсутності правового статусу транзакції з криптовалютами залишаються поза правовим регулюванням і контролем на державному рівні. В результаті з'являється можливість використовувати криптовалюти в нелегальних схемах відходу від податків, виведення капіталу, легалізації (відмиванні) прибутків, отриманих злочинним шляхом, фінансування тероризму, торгівлі наркотиками, людьми і зброєю;

— розробка і впровадження вітчизняної технології «блокчейн». На основі «блокчейн» сьогодні почали створювати відкриті реєстри, в яких фіксується і зберігається інформація про торгові угоди і операції, зобов'язання і права і ін. При цьому верифікація названих реєстрів забезпечується засобами самої автоматизованої системи;

— створення вітчизняних когнітивних апаратно-програмних систем, у тому числі, для стратегічного і операційного прогнозування, проведення розрахунків, торгівлі цінними паперами і т.д.;

Для нейтралізації перерахованих загроз і викликів цифрової економіки Україні рекомендується, передусім, наслідувати наступні базові принципи забезпечення інформаційної безпеки:

— застосування заходів технічного регулювання, передусім відносно устаткування і комплектуючих, апаратних засобів і програмного забезпечення об'єктів транспорту, енергетики і інших стратегічно важливих об'єктів, а також ключових об'єктів життєдіяльності;

— використання виключно вітчизняних технологій інформаційної безпеки (забезпечення цілісності, конфіденційності, аутентифікації і доступності інформації і процесів її обробки);

— застосування технологій захисту інформації з використанням вітчизняних криптографічних стандартів.

Тільки наслідування згаданих принципів безпеки дозволить своєчасно і якісно вирішити поставлені завдання. У свою чергу, це дозволити: підвищити добробут і якість життя громадян країни шляхом підвищення доступності і якості товарів і послуг, вироблених в цифровій економіці з використанням ІКТ; підвищити міру інформованості і цифрової грамотності; поліпшити доступність і якість державних послуг для громадян; забезпечити національну безпеку в державі.

Список бібліографічних посилань

1. Дубінець В. Що пропонують законопроекти про крипту в Україні та який із них можуть ухвалити [Електронний ресурс] / Вікторія Дубінець. – 2018. – Режим доступу до ресурсу: https://cryptota.com.ua/shcho-proponuiut-zakonoproekty-pro-kryptu-v-ukraini-ta-iakyj-iz-nykh-mozhut-ukhvalyty-ihor-markevych/.

2. Перспективи та перешкоди цифрової економіки в Україні [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://nachasi.com/2018/12/04/startups-which-inspire-us/.

3. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018—2020 роки та затвердження плану заходів щодо її реалізації [Електронний ресурс] // Кабінет міністрів України. – 2018. – Режим доступу до ресурсу: https://www.kmu.gov.ua/ua/npas/pro-shvalennya-koncepciyi-rozvitku-cifrovoyi-ekonomiki-ta-suspilstva-ukrayini-na-20182020-roki-ta-zatverdzhennya-planu-zahodiv-shodo-yiyi-realizaciyi.

УДК 343.9:159.9.075
ІРИНА ВАСИЛІВНА ДЕГТЯРЬОВА
кандидат юридичних наук,
старший інспектор відеокримінального аналізу ГУНП в Харківській області

ВИКОРИСТАННЯ СИСТЕМИ КРИМІНАЛЬНОГО АНАЛІЗУ «RICAS» З МЕТОЮ ПОПЕРЕДЖЕННЯ ТА РОЗКРИТТЯ ЗЛОЧИНУ, ЩО ПОЛЯГАЄ У НЕЗАКОННОМУ ЗАВОЛОДІННІ ТРАНСПОРТНИМИ ЗАСОБАМИ (СТ. 289 КК УКРАЇНИ)

Питання боротьби з незаконними заволодіннями транспортними засобами займає важливе місце у боротьбі зі злочинністю, оскільки, дане правопорушення заподіює суттєву майнову шкоду як окремим громадянам, так і державі загалом. За останні роки намітилась тенденція до зменшення кількості випадків незаконного заволодіння транспортними засобами, але дана обставина не знижує актуальності та суспільної небезпеки цього виду правопорушень.

Проведений кримінальний аналіз злочину, дає підстави стверджувати, що все більшої популярності набувають заволодіння автомобілями імпортного виробництва представницького та бізнес класу з терміном експлуатації до 5 років.

Частіше всього, зазначені злочини вчиняються організованою злочинною групою (далі ОЗГ), до складу якої входять: безпосередні викрадачі транспортних засобів; перевізники; автомобільні слюсарі та механіки, які перебивають номери кузова та двигуна, перефарбовують авто; скупники викрадених авто; скупники згорілих автомобілів із документами; особи, які займаються підробленням чи виготовленням підроблених документів; корумповані працівники правоохоронних органів; розробники спеціальних комп'ютерних програм [2, с. 15].

Злочин вчинюється у декілька етапів: підготовка, вчинення та приховування. Так, на етапі підготовки злочинці підшукують автомобіль (певної марки, кольору, року випуску тощо), ретельно стежать за власником, за місцями його паркування, маршрутами пересування, визначають та готують відповідні технічні засоби. Після чого, виготовляють підроблені документи або придбають документи на автомобілі, які були знищені в результаті нещасних випадків чи злочинів (згорілі, втоплені, пошкоджені в результаті ДТП до стану неможливості подальшого використання) з метою подальшого використання відомостей про номери кузова чи двигуна для їх перебивання на викраденому авто. Члени ОЗГ можуть вступити у змову з власником авто певної марки та придбати у нього документи. В подальшому власник звертається до правоохоронних органів про втрату чи викрадення документів. А у злочинців залишаються документи на авто без ознак матеріальної підробки. Як правило, зазначені документи використовуються для легалізації автомобілів аналогічних характеристик. Таким чином з'являються «автомобілі-двійники».

Далі, готують номерні знаки (виготовляють підроблені або використовують від інших автомобілів), усувають перешкоди для виконання запланованого.

Етап викрадення авто займає від 2 до 5 хвилин.

Викрадений автомобіль може бути реалізований наступними способами:

- автомобіль відразу переганяється у певний регіон та продається без документів за півціни заздалегідь визначеним особам. Близько 90 % зазначених авто вивозяться за межі держави, частіше за все у колишні республіки СРСР;
- автомобіль переганяють у так званий «відстійник» (СТО, гаражні кооперативи тощо), розташований неподалік від місця заволодіння транспортним засобом, де авто перефарбовують, змінюють номери агрегатів та за підробленими документами продають як повністю укомплектований автомобіль;
- автомобіль повертають власнику «за винагороду», яка складає 50 % вартості викраденого авто.

Відділом кримінального аналізу ГУНП в Харківській області на постійній основі здійснюється детальний аналіз злочинів, пов'язаних з незаконним заволодінням транспортними засобами та на його основі надаються практичні рекомендації у відповідні підрозділи поліції, з метою запобігання та якісного розкриття злочинів зазначеного виду.

Дослідження проводиться з використанням найновітнішої інформаційної системи кримінального аналізу – «RICAS». В даній системі в реальному часі географічно відображаються злочини, що полягають у незаконному заволодінні транспортними засобами на території м. Харкова та області. Система дозволяє повноцінно здійснювати аналіз: визначити загальну кількість кримінальних правопорушень загалом по області чи окремо по місту, у разі необхідності – окремо по районам; здійснити вибірку злочинів за певний період; провести дослідження за марками авто та визначити ті, які користуються найбільшим попитом серед злочинців; визначити місця найбільшої концентрації злочинів; провести часовий аналіз – пора року, місяць, день тижня, час доби, які найбільш придатні для вчинення злочину; визначити найбільш придатні місця для вчинення злочинів; вивести на карту місця розташування камер відео спостереження, СТО чи гаражних кооперативів, поблизу місця заволодіння транспортним засобом, з метою встановлення можливого місця знаходження автомобіля [3, с. 26].

Зазначене вище можна відобразити на прикладі аналізу, зробленого за 10 місяців поточного року. Так, за вказаний період, в Харківській області всього було зареєстровано 234 заяв та повідомлень про факти викрадення транспортних засобів, з яких окремо на території м. Харкова – 110.

Ілюстрований фрагмент концентрації злочинів, пов'язаних з незаконним заволодінням автотранспорту за допомогою системи «RICAS» чітко демонструє тенденцію розповсюдження цих правопорушень по місту протягом 2018 року (рис.1). Переважна кількість кримінальних правопорушень вчиняється на території таких районів Харкова як

Шевченківський, Московський та на межах Слобідського з Немишлянським й Холодногірського з Новобаварським. Більше всього незаконно заволодівають автотранспортом поблизу жилих будинків та зі стихійних парковок у нічний та вечірній час.

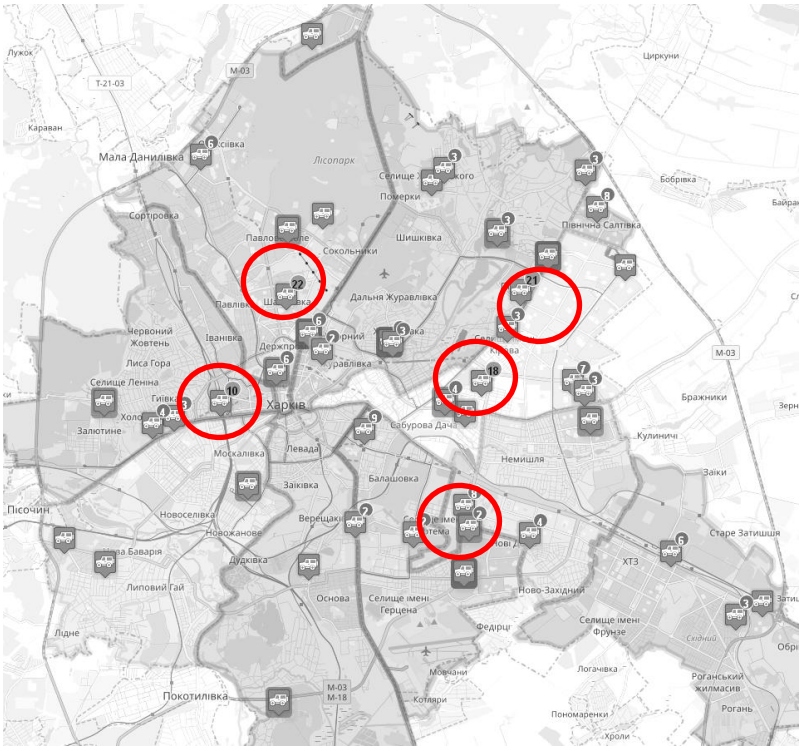


Рис. 1. Місця концентрації кримінальних правопорушень, пов'язаних з незаконним заволодінням транспортних засобів з початку 2018 року на території міста

Як видно з діаграми (рис. 2), відмічається зростання кількості зареєстрованих злочинів у травні та у вересні.

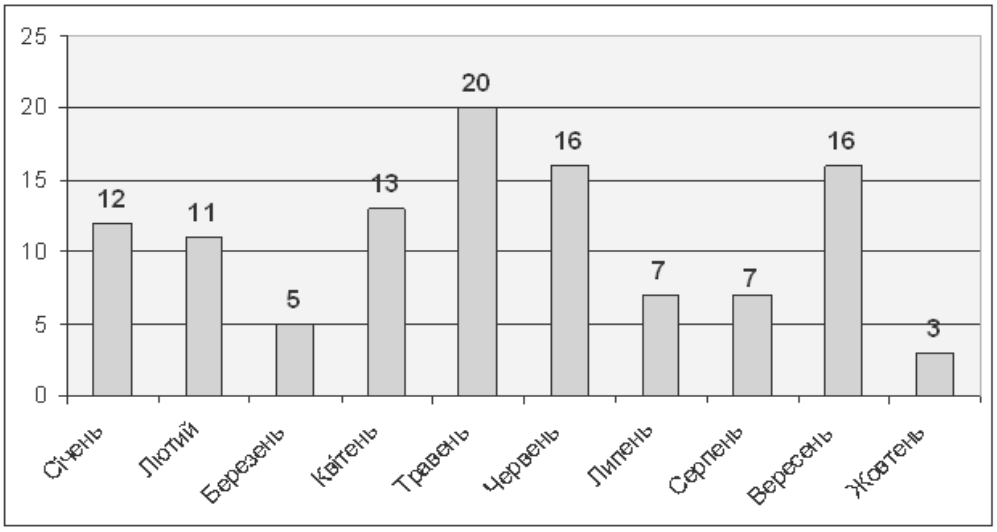


Рис. 2. Кількість викрадень легкового транспорту на території м. Харкова за 10 міс. 2018 року

Співвідношення викрадення легкових автомобілів конкретних марок виробників наведено на діаграмі рис. 3:

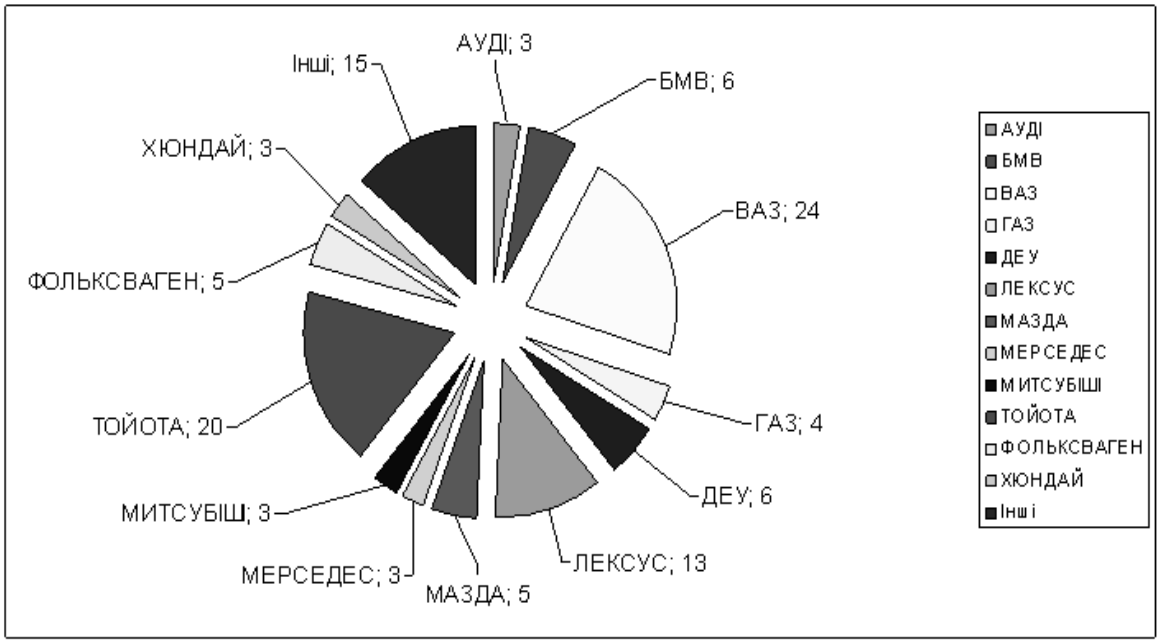


Рис. 3. Співвідношення викрадень по маркам авто

Співвідношення викрадення легкових автомобілів у розрізі пори доби та за днями тижня відображено на діаграмах рис. 4 та рис. 5.

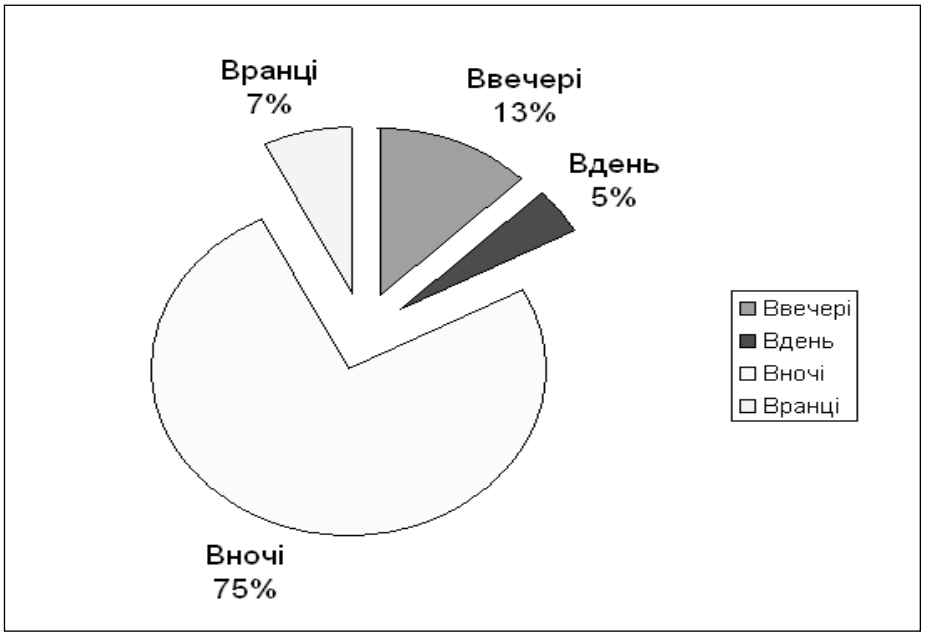


Рис. 4 Співвідношення викрадень по часу доби

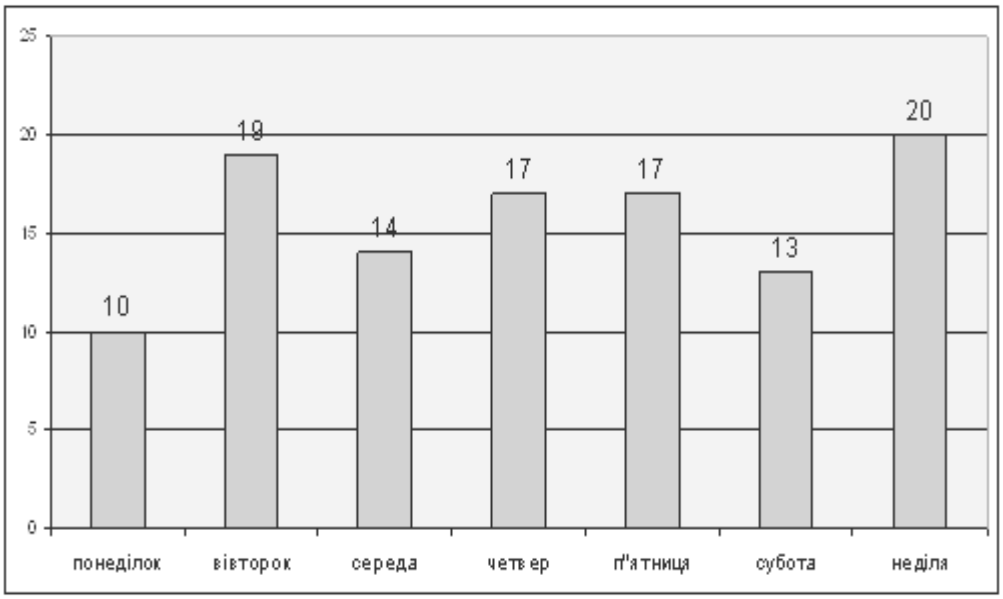


Рис. 5. Кількість викрадень по днях тижня

Система кримінального аналізу дозволяє вивести на карту камери відеоспостереження, які розташовані по місту та навіть в реальному часі відслідковувати пересування транспортного засобу (у разі необхідності оперативного реагування) чи надати інформацію про місця розташування відео записуючих пристроїв, що працюють у режимі запису поблизу місця вчинення злочину (з метою перегляду відеоінформації у записі) (рис. 6).

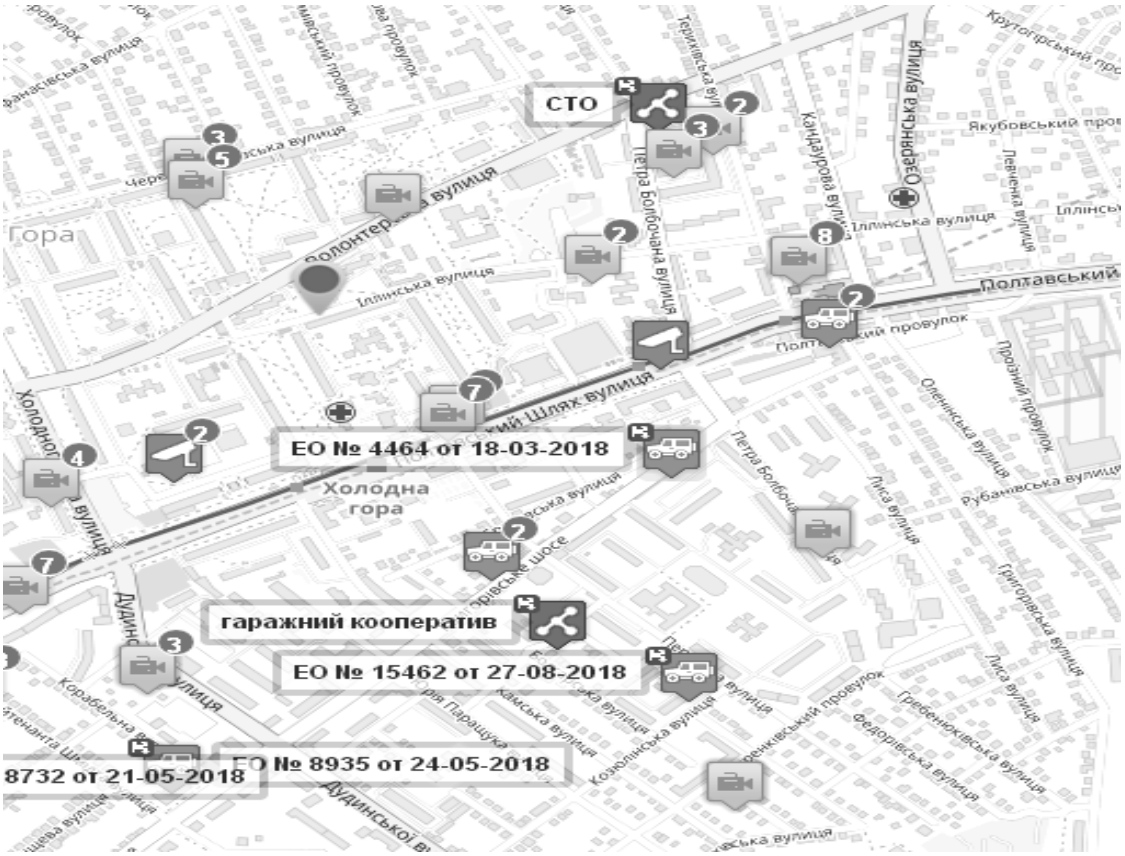


Рис. 6 Картографічне відображення місць розташування відео записуючих пристроїв, СТО та гаражних кооперативів по відношенню до місць вчинення злочинів

У кожному окремому випадку аналітик має можливість надати інформацію про камери відеоспостереження, СТО та гаражні кооперативи, що розташовані поблизу місця вчинення злочину. Огляд записів з камер зовнішнього відео спостереження, в поле зору яких потрапило місце знаходження викраденого автомобіля, процес незаконного заволодіння ним, та маршрут можливого пересування після злочину, значно полегшує процес розслідування злочину. Інформація щодо знаходження СТО та гаражних кооперативів поблизу місця заволодіння транспортним засобом, дає підстави оперативним працівникам перевірити їх невідкладно та першочергово.

Отже, як видно з наведеного прикладу, інформація, отримана аналітиком з системи кримінального аналізу «RICAS» відображає повну характеристику злочину, що полягає у незаконному заволодінні транспортним засобом. В подальшому зазначена інформація використовується не лише слідчими підрозділами поліції з метою розкриття злочину, а й підрозділами превентивної діяльності з метою розстановки нарядів поліції по місту у місцях найбільшої концентрації злочинності, з метою попередження вчинення суспільно-небезпечного діяння зазначеного виду.

Список використаних джерел

1. Кримінальний кодекс України: від 05.04.2001 [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua/laws/show/2341-14
2. Незаконне заволодіння транспортними засобами, особливості досудового розслідування: науково-методичні рекомендації. – Харків : ХНУВС, 2015. – 46 с.
3. Прикладний кримінальний аналіз на базі інформаційно-аналітичної системи «RICAS»: методичні рекомендації щодо аналітичної діяльності та кримінального аналізу на базі інформаційно-аналітичної системи «RICAS». – Харків : «Юрайт», 2018. – 92 с.

УДК 004.9 +343.1

ВІТАЛІЙ ВІКТОРОВИЧ НОСОВ
кандидат технічних наук, доцент,
професор кафедри кібербезпеки факультету № 4
Харківського національного університету внутрішніх справ

ВИКОРИСТАННЯ АСОЦІАТИВНИХ КАРТ В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ

В структурі Національної поліції України на всіх рівнях (центральному, міжрегіональному і територіальному) функціонує достатньо велика кількість аналітичних підрозділів, наприклад [1]:

– Центральний орган управління:

- Департамент організаційно-аналітичного забезпечення та оперативного реагування;

- Департамент інформаційно-аналітичної підтримки;
- Управління кримінального аналізу;

– Департамент патрульної поліції:
- управління моніторингу та аналітичного забезпечення;

– Департамент внутрішньої безпеки:
- управління моніторингу та аналізу;

– Департамент кіберполіції:
- відділ аналітичного забезпечення;

– Департамент захисту економіки:
- відділ оперативно-аналітичного забезпечення;

– Департамент поліції охорони:
- управління організаційно-аналітичного забезпечення та оперативного інформування.

Завданням аналітичних підрозділів в широкому розумінні є на першому етапі пошук, відбір, накопичення, узагальнення і збереження певних інформаційних одиниць, а на другому - виробництво на підставі наявних інформаційних одиниць і складних розумових процесів нового знання щодо явища або події відповідної сфери компетенції. Другий етап формування нового знання є доволі складним і може бути технологічно спрощений візуалізацією відносин між інформаційними одиницями цілого. Для цього доцільно використовувати так звані асоціативні карти або mind map tools (ММТ), які є комп'ютерним програмним забезпеченням побудови в радіальній, нелінійній формі деревовидних (із можливими зв'язками між гілками) діаграм зв'язків між одиницями інформації.

Існуючі рішення ММТ відрізняються між собою багатьма параметрами, серед яких:

– коштовність або безкоштовність;
– онлайн доступ до веб сервера ММТ або автономна робота;
– платформа (Mac, Linux, Windows);
– легкість у використанні;
– естетичність відображення;
– наявність різноманітних шаблонів діаграм;
– опції імпорту/експорту результатів;
– можливість сумісної роботи (collaboration).

В [2-8] здійснено порівняльний аналіз і ранжування ММТ за різними критеріями. Якщо взяти тільки параметр безкоштовності (free), то можна зазначити такі, найбільш популярні ММТ: Edraw Mind Map, Docear, FreeMind, Freeplane, VUE, WiseMapping, Coggle, Mind42, Xmind, 3D Topicscape.

Для впровадження ММТ у діяльність аналітичних підрозділів поліції потрібно відібрати типові кейси створення нових знань у сфері їх компетенції, підібрати відповідні, найбільш підходящі, рішення ММТ та розробити методики їх застосування. Відібрані ММТ із методиками їх застосування доцільно включити у навчальний процес підготовки бакалаврів з кібербезпеки у вибірковий блок дисциплін кримінальної розвідки Харківського національного університету внутрішніх справ.

Список використаних джерел:

1. Офіційний сайт Національної поліції. URL: https://www.npu.gov.ua/about/struktura/struktura/ (дата звернення 4.12.2018).
2. Christopher McFadden. 17 of The Best Mind Mapping Tools (Online, MacOS and Windows). Posted on September, 08th 2018. URL: https://interestingengineering.com/17-of-the-best-mind-mapping-tools-online-macos-and-windows (дата звернення 4.12.2018).
3. Clifford Chi. 11 of the Best Mind Mapping Software to Brainstorm Better Ideas. Originally published Aug 28, 2018 6:00:00 AM, updated October 08 2018. URL: https://blog.hubspot.com/marketing/best-mind-mapping-software (дата звернення 4.12.2018).
4. Saikat Basu. 8 Free Mind Map Tools & How to Best Use Them. Posted on November 27, 2015. URL: https://www.makeuseof.com/tag/8-free-mind-map-tools-best-use/ (дата звернення 4.12.2018).
5. Kenneth Kimari. 12+ best mind mapping tools to organize your thoughts and ideas. Posted on March 9, 2018. URL: https://windowsreport.com/mind-mapping-tools-software/ (дата звернення 4.12.2018).
6. Top 29 free & premium mind mapping software. URL: https://www.predictiveanalyticstoday.com/top-free-premium-mind-mapping-software (дата звернення 4.12.2018).
7. Best 20 mind mapping software of 2018. URL: https://financesonline.com/mind-mapping/ (дата звернення 4.12.2018).
8. Nate Drake. Best mind map software of 2018. Posted on June 12, 2018. URL: https://www.techradar.com/news/best-mind-map-software (дата звернення 4.12.2018).

УДК 004.021

ЄВГЕН МИКОЛАЙОВИЧ ГРІНЧЕНКО
кандидат технічних наук, доцент, старший науковий співробітник Науково-дослідної лабораторії захисту інформації та кібербезпеки Харківського національного університету внутрішніх справ
ЗАХАР ГРИГОРОВИЧ ДЕМИДОВ
науковий співробітник Науково-дослідної лабораторії захисту інформації та кібербезпеки Харківського національного університету внутрішніх справ
ОЛЕГ ОЛЕКСАНДРОВИЧ КОЛМИК
науковий співробітник Науково-дослідної лабораторії захисту інформації та кібербезпеки Харківського національного університету внутрішніх справ

ДЕЯКІ АСПЕКТИ РОЗРОБКИ ІНФОРМАЦІЙНОЇ СИСТЕМИ УПРАВЛІННЯ КАДРОВОГО ЗАБЕЗПЕЧЕННЯ ПІДРОЗДІЛІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Кадрове забезпечення підрозділів Національної поліції України є одним із пріоритетних напрямів удосконалення управлінської діяльності, адже від рівня професіоналізму та компетентності, пильності, правової культури,

службової етики, чесності, порядності співробітників, їх готовності та здатності стояти на варті закону багато в чому залежить авторитет органів Національної поліції України.

Велика кількість особового складу підрозділів Національної поліції України, різноманітність їх підпорядкування призвела до значного ускладнення процедури управління кадровим потенціалом. Одним з напрямків вирішення цього вельми складного питання є використання комп'ютерної техніки та відповідного програмного забезпечення. Нагальним питанням є створення інформаційної системи управління кадрового забезпечення підрозділів Національної поліції України.

Інформаційна система управління - це сукупність математичних і економічних методів, інформації, програмно-технічних і технологічних засобів і компетентних фахівців, основною метою яких є обробка інформації та прийняття управлінських рішень. Відзначимо, що реалізація інформаційних систем неможлива без комп'ютерних технологій. ІКТ зі всілякими спеціалізованими програмами є технічною базою реалізації даної системи. Головним завданням інформаційно технічних систем в управлінні персоналом є виявлення причинно-наслідкових зав'язків між процесами взаємодії і результатами.

Функція управління персоналом на різних рівнях - розробка рішень і контроль за їх реалізацією. Необхідність реалізації цих рішень і включає інформаційний процес в систему управління персоналом, так як її основними функціями є отримання, передача, обробка, зберігання, використання інформації на рівні всіх ступенів ієрархічної системи організації. Інформаційне забезпечення системи управління персоналом являє сукупність поставлених рішень за обсягом, розміщення і формам організації інформації, постійно знаходиться в системі управління при її функціонуванні. Воно включає оперативну інформацію, нормативно-довідкову інформацію, класифікатори техніко-економічної інформації та внутрішні системи документації.

Всі ІС управління персоналом використовують необхідну інформацію для якісного та ефективного виконання стратегічних, тактичних і оперативних завдань кадрового менеджменту. Але найчастіше, такі системи зберігають особисту інформацію про співробітників, а також здійснюють формування різних бланків і звітів на співробітника. Таким чином, характеризуючи особливості функціонального спектра інформаційних систем для управління персоналом ми можемо виділити ряд конкретних груп функцій ІС.

1) Група функцій ІС «Облік відомостей про персонал» Перша група функцій інформаційних систем дозволяє здійснювати всебічний облік персоналу з найрізноманітніших критеріям, починаючи від стандартних відомостей і закінчуючи рівнем професійної компетентності. Іншими словами - формувати персональне «портфоліо» того чи іншого працівника, яке можна використовувати в подальшому для визначення його потреб, очікувань, розробки персональної програми навчання, просування по кар'єрі і т.д.

2) Група функцій ІС «Облік діяльності персоналу» Сучасні інформаційні системи дозволяють враховувати результати трудової

діяльності співробітників - конкретні факти виконання трудових норм, показники якості трудової діяльності та інші.

3) Група функцій ІС «Перестановки персоналу» До числа можливостей інформаційних систем відносять і можливість обліку перестановок персоналу всередині організації, відображення системи внутрішніх корпоративних комунікацій - того, як між собою взаємодіють окремі співробітники.

4) Група функцій ІС «Навчання персоналу» На основі враховуються ІС показників трудової діяльності і компетентності співробітників сучасні ІС можуть дозволяти формувати індивідуальну траєкторію професійного розвитку співробітників.

5) Група функцій ІС «Мотивація і стимулювання праці персоналу» Також, ІС можуть здійснювати зберігання та облік даних про особистісні особливості співробітників, їх мотиви, стимули, потреби та очікування - всього того, що дуже важливо в процесі мотивації персоналу.

Створення такої інформаційної системи відбувається в науково-дослідній лабораторії захисту інформації та кібербезпеки Харківського національного університету внутрішніх справ.

УДК 004.932

МИКОЛА ВОЛОДИМИРОВИЧ МОРДВИНЦЕВ
кандидат технічних наук, доцент, провідний науковий співробітник Науково-дослідної лабораторії захисту інформації та кібербезпеки Харківського національного університету внутрішніх справ
ОЛЕКСІЙ ВОЛОДИМИРОВИЧ ХЛЄСТКОВ
старший науковий співробітник Науково-дослідної лабораторії захисту інформації та кібербезпеки Харківського національного університету внутрішніх справ
СЕРГІЙ ПАВЛОВИЧ НИЦЮК
старший науковий співробітник Науково-дослідної лабораторії захисту інформації та кібербезпеки Харківського національного університету внутрішніх справ

ДЕЯКІ АСПЕКТИ ВИКОРИСТАННЯ АВТОМАТИЗАЦОВАНИХ СИСТЕМ ВІДЕОДОКУМЕНТУВАННЯ ПЕРЕМІЩЕНЬ ОБ'ЄКТА В ПОЛІЦЕЙСКІЙ ДІЯЛЬНОСТІ

Розглядаються деякі аспекти використання система відеодокументування переміщень об'єкта в поліцейській діяльності з використанням системи геолокації GSM оператора та GPS навігації

Все більше в поліцейській діяльності використовуються системи відеоспостереження. Запровадження систем відеоспостереження стає дуже важливим напрямом забезпечення безпеки громадян в містах і в великих селах. А за рахунок того що збільшується кількість веб-камер, які застосовують, як

правоохоронними органами так і комерційними організаціями вирішення задачи безпеки населення стає більш ефективним.

Досвід країн Європейського Союзу та США показує що використання систем відеоспостереження значно сприяє оперативності реагування на правопорушення, швидкому встановленню осіб, які їх здійснюють, запобігання терористичним актам, пошук свідків правопорушень.

Наявність подібних систем є стримуючим чинником для правопорушника, навіть за відсутності співробітника правоохоронних органів[1, с. 54].

На думку поліції, використання систем відеоспостереження в громадських місцях дозволить зменшити кількість правоохоронців на вулицях і при цьому зробить їх роботу більш ефективною.

В доповіді пропонується спосіб відео документування за допомогою засобів відео фіксації, при цьому відбувається порівняння координат об'єкта, що має мобільний телефон або GPS навігатор із зоною спостереження відеокамери, і автоматичне об'єднання фрагментів появи об'єкта в зоні видимості в один відеозвіт.

В даний час є всі технічні можливості для розробки і впровадження системи автоматичного створення відеозвітів (САСВ) за допомогою IP - камер.

Пропонується створення САСВ[2, с. 54], в результаті якої правоохоронні органи зможуть отримати автоматично створений відеозапис про діяльність об’єкту спостереження. У той же час держава отримує можливість поліпшити систему безпеки при проведенні масових заходів.

САСВ має три складових: система панорамної зйомки, система ближньої зйомки, система індивідуальної зйомки.

Система панорамної і ближньої зйомки припускає встановлення IP-камер на вулицях, майданах, в великих будівлях, стадіонах. При цьому встановлюється два види камер: ближньої і дальньої зйомки. Камери далекої зйомки документують панорамну картинку, в яку потрапить об’єкт спостереження, а камери ближньої зйомки виробляють зйомку в зоні своєї видимості на малій відстані. Останні доцільно встановлювати, як на вулицях , так і в приміщеннях.

Для того щоб отримати відео звіт про діяльність об’єкту спостереження правоохоронні органи замовляють цю послугу у мобільного оператора. Вказуючи номер мобільного телефону об’єкта спостереження. Мобільний оператор визначає точне положення об’єкта і сектор спостереження тієї чи іншої IP-камери за певною програмою записує відео фрагмент, коли об’єкт перебуває в зоні зйомки тієї чи іншої камери. Переходячи із зони зйомки від однієї камери до іншої, комп'ютерна програма монтує ці фрагменти в один фільм. Чергування фрагментів камер ближнього спостереження з фрагментами панорамних камер створить більш повне сприйняття переміщень об'єкта. Перемикання на панорамну IP-камеру відбувається при виході об'єкта із зони спостереження ближньої IP-камери.

Система індивідуальної зйомки передбачає доповнення створюваного фільму-звіту фрагментами індивідуальної IP-камери. Для цього особа яка веде спостереження повинна мати IP-камеру якщо існує покриття Wi-Fi, або камеру,

сполучену з мобільним телефоном по якому передавати відео потік. При цьому фрагменти індивідуальної IP-камери через засоби мобільного оператора або через Wi-Fi канали зв'язку будуть автоматично вмонтовані у фільм-звіт.

Розглядаються напрямки використання видеофіксації переміщень об'єкта.

Перше це спостереження за об'єктом. Другий напрям це збір доказової бази присутності об'єкта в даному місті в даний час. Яка може бути використана як для звинувачення підозрюваного, так і для його захисту. Третій напрям це пошук свідків подій. Які мають мобільні телефони і знаходились в полі зору веб-камери.

Висновки:

Удосконалення системи відеоспостереження дозволяє більш ефективно реалізовувати роботу правоохоронних органів. Система дозволить підвищити ефективність діяльності поліції.

Система запатентована автором: Мордвинцев М.В., Машкаров Ю.Г. Спосіб відео документування переміщень об'єкта за допомогою системи відео фіксації. Патент на корисну модель № 73635, 2012, -4 с.

Список бібліографічних посилань

1. Мордвинцев Н.В., Усовершенствование систем видеонаблюдения при реализации задач правоохранительных органов. Издательский дом "Интернаука" Международный научный журнал 5 (1), 59-61
2. Мордвинцев М.В., Машкаров Ю.Г. Спосіб відео документування переміщень об'єкта за допомогою системи відео фіксації. Патент на корисну модель № 73635, 2012, -4 с.

ОЛЕГ СТЕПАНОВИЧ ГАВРИШ
викладач кафедри економічної та інформаційної безпеки
Дніпропетровського державного університетету внутрішніх справ

ІНФОРМАЦІЙНІ АСПЕКТИ СУЧАСНИХ МЕТОДІВ ГІБРИДНОЇ ВІЙНИ

Основна проблема гібридної війни полягає в тому, що вона не закінчується швидко. У кіберпросторі ми повинні готуватися до тривалої війни. Більш того, засоби і методи ведення гібридної війни будуть удосконалюватися з боку противника. Потрібно залучати кращих інформаційних фахівців до цього процесу і воювати кращими методами в тісній співпраці з нашими західними партнерами. Тому що застарілими методами виграти сучасну інформаційну війну неможливо [1].

Ситуація безпеки навколо України може змінюватися динамічно. Очевидно, що в разі її загострення і виникнення значних інформаційних загроз будуть швидко прийняті необхідні політичні та управлінські рішення, затверджені нормативно-правові акти. Але, все це втрачає будь-який сенс, якщо в Україні завчасно і в необхідній кількості не будуть відібрані і

підготовлені бійці «інформаційного фронту», які вміють ефективно виконувати завдання в області кібербезпеки держави.

Аналіз ситуації показав картину, яка насторожує. На тлі поточного дефіциту справжніх фахівців ми виявили тенденцію відтоку навіть наявних кадрів. Не секрет, що в кінці минулого року звільнився в запас полковник Владислав Селезньов, який заслужив гарну репутацію серед представників ЗМІ та симпатії у численних аудиторій глядачів. Стало відомо про наміри звільнитися в запас добре відомого в закритих колах офіцера структур інформаційно-психологічних операцій, який реалізував успішний проект з протидії російської інформаційної агресії. Є інші аналогічні приклади. Отже, щось у нас не так і проблема кадрового потенціалу стає критичною. Тому потрібно щось кардинально змінювати [1].

Нещодавно натрапила на інформацію з питань підготовки та мотивації фахівців для дій в інформаційному та кіберпросторі в західних країнах. Виявляється, у них є суттєві і іноді дуже схожі з нашими проблеми. Російська інформаційна агресія також спонукала їх до перезавантаження, а в кадровому плані виникло найбільше запитань. Наприклад, ЦРУ в 2017 році був змушений відкрито оголосити про пошук значної кількості нових фахівців, які добре знають російську мову, відповідну культуру, традиції і т.д. і готові внести свій внесок у протидію деструктивним діям Російської Федерації в інформаційному просторі.

Майже одночасно спецслужба в Великобританії GCHQ (Government Communications Headquarters, тобто «Центр урядових комунікацій») була змушена визнати, що відчуває проблеми з залученням, мотивацією і змістом персоналу, в першу чергу фахівців з інформаційної безпеки (згідно з матеріалами щорічного звіту GCHQ). Причина дуже проста - урядова організація не в змозі бути конкурентною з високотехнологічними компаніями сфери бізнесу, які мають набагато більше важелів мотивації і часто пропонують в кілька разів більший рівень грошового забезпечення.

У сусідній Польщі також змушені підвищувати імідж спецслужб і одночасно вирішувати їх кадрову проблему через відкриті джерела інформації.

Подібних прикладів досить багато. Їх об'єднує одне: існує кадрова проблема, але одночасно з'являється її розуміння і бажання вирішити. Ми повинні бути вдячними, оскільки досвід сусідів дає нам шанс не «винаходити велосипед» або «наступати на граблі». У нас, в свою чергу, виявляються цілком очікувані причини проблем.

Перша і найголовніша - це неповне розуміння нових викликів в інформаційному просторі і шляхів нейтралізації їх з боку вищого політичного і військового керівництва країни. Це окрема тема для дискусії, тому залишимо її за межами цієї публікації.

Наступна проблема - процедури підготовки кадрів в навчальних закладах і подальше призначення їх після випуску на конкретні посади в силовому блоці. Виявляється, після майже чотирьох років війни ми зберігаємо якесь зачароване коло. Підготовка фахівців у вищих навчальних закладах для структур сектору безпеки і оборони здійснюється на підставі державного

замовлення. Процедура формування такого замовлення, в першу чергу, ґрунтується на штатній потребі у фахівцях певного рівня і напряму на момент їх випуску для подальшої служби в конкретних організаційних структурах (певних підрозділах спецслужб, бойових військових частинах і т.д.). Іншими словами, якщо ми очікуємо через 5 років конкретного лейтенанта-випускника, то вже сьогодні ми повинні розуміти, на яку конкретно посаду ми його призначаємо. А якщо ці посади ще не існують? Тоді в нинішньому державному замовленні ці фахівці просто не будуть передбачені і набір першокурсників не відбудеться.

Тому виникає питання, чи існує в державі чітке бачення перспективних організаційних структур? Чи не чергових департаментів або директоратів на управлінської верхівки силових структур, а саме бойових підрозділів? До речі, я знаю про низку рішень в силових структурах щодо вдосконалення та розвитку структур інформаційного протиборства, які чомусь не виконані.

Третя проблема - де і як готувати фахівців? Мені добре відома і зрозуміла проблематика стратегічних комунікацій. Наприклад, кілька років тривала дискусія про необхідність створення в Національному університеті оборони України навчально-наукового підрозділу у напрямку стратегічних комунікацій, який мав унікальний шанс стати загальнодержавним інтегратором серед силових структур держави та прикладом навіть для західних партнерів. За наявною інформацією цю ідею чомусь «спустили на гальмах» і в перспективній структурі університету такий підрозділ не розглядається.

Потрібні й інші гнучкі форми кадрового забезпечення «інформаційного фронту». Наприклад, через службу в резерві для цивільних представників сфери ЗМІ, рекламного бізнесу, відомих блогерів, «білих хакерів» і ін. Про всяк випадок, в Збройних силах України вже більше 150 000 чоловік служать в оперативному резерві і логічно бачити в їх рядах бійців інформаційного напряму.

Найголовнішим фактором успіху я вважаю питання формування цінностей, етичних норм і мотивації. Більшість необхідних спеціальностей інформаційних воїнів є високотехнологічними і добре стимульований матеріально в цивільному житті. Це не солдати піхоти, які можуть вчитися в масовому форматі в разі мобілізації. Йдеться про штучний підхід. Кожен такий фахівець є унікальним і своєрідним. Якщо ми сподіваємося отримати їх досвід і знання для безпеки держави - слід міняти наші підходи в роботі державних структур з цінними кадрами і фахівцями [2].

Здається, що нам достатньо грати в волонтерські «інформаційні війська». Досить «виїжджати» на волонтерських проектах і випрошувати допомогу у закордонних партнерів. Настає час вирішувати питання протидії інформаційному агресору на професійному рівні. Або іншими словами - інвестувати в майбутнє безпеки держави.

Використані джерела

1. Попова Т. Методами "красных замполитов" выиграть современную информационную войну невозможно. [Електронний ресурс] // NV.UA – 2018.

– Режим доступу: https://nv.ua/opinion/popova/hlavnaja-problema-informatsionnoho-fronta-ukrainy-2450161.html

2. Колодюк А. Информационные технологии: двигатель для Украины. [Електронний ресурс] // ZN.UA – 2018. – Режим доступу: https://zn.ua/ECONOMICS/informatsionnye_tehnologii_dvigatel_dlya_ukrainy.html

ЕДУАРД ВОЛОДИМИРОВИЧ РИЖКОВ
кандидат юрідичниїх наук, доцент, завідувач кафедри економічної та інформаційної безпеки, Дніпропетровського державного університету внутрішніх справ

ДЕЯКІ ПРОБЛЕМНІ ПИТАННЯ В РОБОТІ СЕКТОРІВ ІНФОРМАЦІЙНОЇ ПІДТРИМКИ ТЕРИТОРІАЛЬНИХ ОРГАНАХ ТА ПІДРОЗДІЛАХ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ

Відповідно до п. 2 ст. 18 Закону України «Про національну поліцію» поліцейський повинен професійно виконувати свої службові обов'язки відповідно до вимог нормативно-правових актів, посадових (функціональних) обов'язків, наказів керівництва. На практиці з реалізацією цих норм закону виникають проблеми, адже відсутній єдиний підхід до організації покладання службових обов'язків на працівників відділів та відділень поліції.

Так як специфіка роботи співробітника сектору інформаційної підтримки (далі – СІП) управління та районного відділу різниться, то й функціональні обов'язки мають бути різними. Проте це не виключає системності в підході до складання функціональних обов'язків для співробітників. З метою більш якісного виконання покладених функцій вони мають бути вичерпними та чітко визначеними. Адже зараз та робота, яку виконують працівники, залежить в певній мірі від особистого ставлення керівника відділу чи відділення, що знижує ефективність кінцевого результату.

Виходом з ситуації що склалася нами вбачається необхідність розробки типових функціональних обов'язків на рівні Департаменту інформаційно-аналітичної підтримки для працівників кожного рівня підрозділів з урахуванням їх специфіки та покладених на них завдань. Це забезпечить більш ефективне та стабільне виконання завдань підрозділами на місцях та зменшить навантаження на працівників «не своєї» роботи, що в свою чергу підвищить якість кінцевого результату.

На рівні управлінь, як на нашу думку, пропонуємо визначити доступи виключно до тих інформаційних підсистем, які необхідні для виконання покладених обов'язків. Наприклад, великою проблемою є навантаження окрім основної інформаційної підсистеми, яка підлягає наповненню - ІП «Кримінальна статистика», є ведення ІП «Єдиний облік», а саме облік та контроль прийнятих рішень за матеріалами, які розглянуті відповідно до Закону України «Про звернення громадян».

Проблемним питанням також залишається залежність працівників та їх робочого часу від внесення даних до ЄРДР. На практиці це залежить від

багатьох факторів: роботи слідчого, прокурора, інших чинників. При цьому, результати діяльності в загальний показник рахуються за загальним принципом по завершенню доби. Пропонується обмежити можливість внесення показників після закінчення робочого дня.

Також викликає незадоволення рівень матеріально-технічного забезпечення, на місцях відсутнє у повній мірі забезпечення комп'ютерною та копіювальною технікою, іншими витратними матеріалами.

Однією з актуальних проблем є невідповідності між ІП «Кримінальна статистика» та ЄРДР, що призводить до невідповідності між ними. Проте відповідно до доручення статистика має відповідати ЄРДР. Логіка у кожної підсистеми різниться, що додає невідповідності.

Ці питання потребують свого вирішення на етапі переходу підрозділів Департаменту інформаційно-аналітичної підтримки Національної поліції до оновленого формату, що передбачає більшу централізацію у питанні експлуатації баз даних та започаткування піврічної первинної підготовки до працівників низової ланки секторів інформаційної підтримки.

УДК 004.738

ВІТАЛІЙ АНАТОЛІЙОВИЧ СВІТЛИЧНИЙ,
кандидат технічних наук, доцент кафедри кібербезпеки, факультету №4
Харківського національного університету внутрішніх справ

АКТУАЛЬНІ ПИТАННЯ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧА У МЕРЕЖІ ІНТЕРНЕТ

Однією з проблем з якою стикається працівник поліції при розслідувані злочинів, які були здійсненні через мережу Internet є визначення комп'ютера користувача з якого були здійснені кримінальні дії (кіберзлочини). Погрішність ідентифікації, заснованої на IP-адресі, складається з погрішностей передачі і погрішностей користування комп'ютером. Так, наприклад, при роботі користувачів через ргоху-сервер уся мережа, яка за ним ховається, у більшості випадків матиме єдиний IP-адрес. З іншого боку, працюючи через комутоване з'єднання, користувач при кожному підключенні отримуватиме від провайдера новий IP-адрес і т. д.

Завдання ідентифікації користувача не втрачає своєї актуальності в зв'язку постійною гонкою технологій захисту інформації і технологій неправомірного отримання доступу до інформації. Актуальність цього завдання для мережі Інтернет підвищується використанням незахищених каналів передачі даних.

Завдання ідентифікації пристрою зазвичай вирішується за допомогою унікальних кодів таких як MAC або IP-адрес в мережах Ethernet або IMEI в мережах GSM. Проте використання унікального коду дає відповідь на питання те ж цей пристрій або ні, але не повідомляє точний тип пристрою і спосіб його використання конкретним користувачем. Окрім ідентифікаторів,

можливе використання додаткової інформації, яка затребувана у разі обробки непрямих ознак, на підставі інформації отримуваної з датчиків пристрою і в результаті роботи програмного забезпечення на пристрої. В даному випадку мається на увазі визначення типу діяльності користувача за даними глобальних систем позиціонування і гіроскопа, а також застосування методів динамічної і статичної біометрії, таких як, рисунок вен на долоні, відбиток пальця, веселкова оболонка ока, геометрія кисті руки або особи, 3D-проекція черепа, клавіатурній почерк, форма вуха, голос і будь-яка інша відмітна ознака може служити для ідентифікації людини біометричною системою.

Використовуємо поняття відбиток пристрою, стосовно інформації що залишається на серверах і інших пристроїв реєстрації, а поняття відбиток особи в пристрої до інформації що побічно характеризує людину за інформацією що залишилася у використаному їм пристрої. Прикладом відбитку пристрою служить запис в log-файлі сервера, а відбитком особи інформація про використані програми, час і тривалість використання програм, набір використаних файлів і інших ресурсів.

Особливе місце серед програмного забезпечення з точки зору завдання ідентифікації пристрою займає браузер, як програма, за допомогою якої користувач дістає доступ до більшості Internet-ресурсів. Для ідентифікації використовується інформація cookies-файлів та інформація про встановлені шрифти і плагіни. Вирішуючи задачу ідентифікації з використанням непрямих ознак, слід враховувати швидкість зміни конфігурацій апаратного і версій програмного забезпечення вживаного користувачем, а так само біологічні ритми до яких схильна людина. Динамічні біометричні ознаки людини змінюються впродовж півроку. Статичні біометричні ознаки зберігаються упродовж усього життя.

Рішення задачі ідентифікації людини і пристрою використовуватиметься при реалізації концепції «програмний агент», для визначення психофізіологічного стану людини і в завданнях з області безпеки, для створення механізмів відстежування шляху. Ідентифікація пристрою і людини є проміжними цілями. Завдяки ідентифікації пристрою можливе калібрування методів знімання інформації. Кінцевою метою ідентифікації' пристрою є ідентифікація людини, отримання прямої або непрямої інформації про нього.

Початковими даними для ідентифікації пристрою і людини пропонується вважати: інформацію про пристрій, інформацію про навколишній світ, інформацію про людину. Складність формалізації початкових даних полягає в неможливості побудови вичерпної безлічі значень деяких ознак. Інформація про використання клавіатури складається з коду клавіші, часу події, типу події. Проте формалізувати ознаку, пов’язану з граматичними і орфографічними помилками, що допускаються користувачем при наборі тексту, як мінімум, складно. Інформація про пристрій складається з: списку і конфігурації використовуваного апаратного забезпечення; списку і конфігурації встановлених програм, і, якщо це можливо, часу установки програм;

інформації збереженої на облаштуванні користувача у вигляді соокіев-файлів, інших тимчасових файлів; відбитку файлової системи пристрою.

Під відбитком файлової системи розуміється інформація про структуру файлової системи, а не отримання математичної свертки даних у файловій системі. Особлива увага приділяється файлам старше за місяць, в яких не відбувалося змін за цей час. Вони мають достатню стабільність, щоб на деякий час стати ідентифікуючою ознакою. Для створення відбитку файлової системи пропонується використовувати інформацію про їх ім'я, місце розташування, розмір, дату створення і дату редагування.

Інформація про користувача складається з: днів тижня, часу доби використання, тривалості активності програмного забезпечення; друкарських помилках, що повторюються, словах паразитах, помилках при наборі тексту; подіях миші або клавіатури.

Кінцевою метою дослідження завдання ідентифікації людини і пристрою є побудова розпізнавана, здатного із задовільною точністю робити ідентифікацію. Особливість цього пристрою полягає в непостійному наборі вхідних значень, що повинне відбиватися на його внутрішній структурі.

УДК 343.9 + 51-77

ОКСАНА ПЕТРІВНА МЕЛАЩЕНКО
старший викладач кафедри інформаційних технологій факультету №4 Харківського національного університету внутрішніх справ
КСЕНІЯ ВОЛОДИМИРІВНА ЮРТАЄВА
кандидат юрідичниїх наук, доцент кафедри кримінального права і кримінології факультету № 1 Харківського національного університету внутрішніх справ

КОРЕЛЯЦІЙНА ЗАЛЕЖНІСТЬ ІНФОРМАТИЗАЦІЇ СУСПІЛЬСТВА ТА РІВНЯ КІБЕРЗЛОЧИННОСТІ

Впровадження електронно-обчислювальної техніки в управлінські процеси та інші сфери життя суспільства сприяло не лише стрімкому розвитку наукової думки та успішному вирішенню багатьох технічних і соціальних проблем, але й призвело до появи нових видів злочинів, зокрема, незаконного втручання в роботу електронно-обчислювальних машин, систем і комп'ютерних мереж, розкрадання, присвоєння, вимагання комп'ютерної інформації, вчинення агресивних злочинів з використанням комп'ютерних технологій тощо. У науці сукупність суспільно небезпечних посягань з використанням комп'ютерної техніки отримало назву кіберзлочинність.

На міжнародному рівні кіберзлочини були криміналізовані у 2001 році Конвенцією РЄ про кіберзлочинність. На національному рівні поняття кіберзлочину отримало закріплення лише нещодавно 5 жовтня 2017 р. у ст. 1 закону України «Про основні засади забезпечення кібербезпеки України» [1].

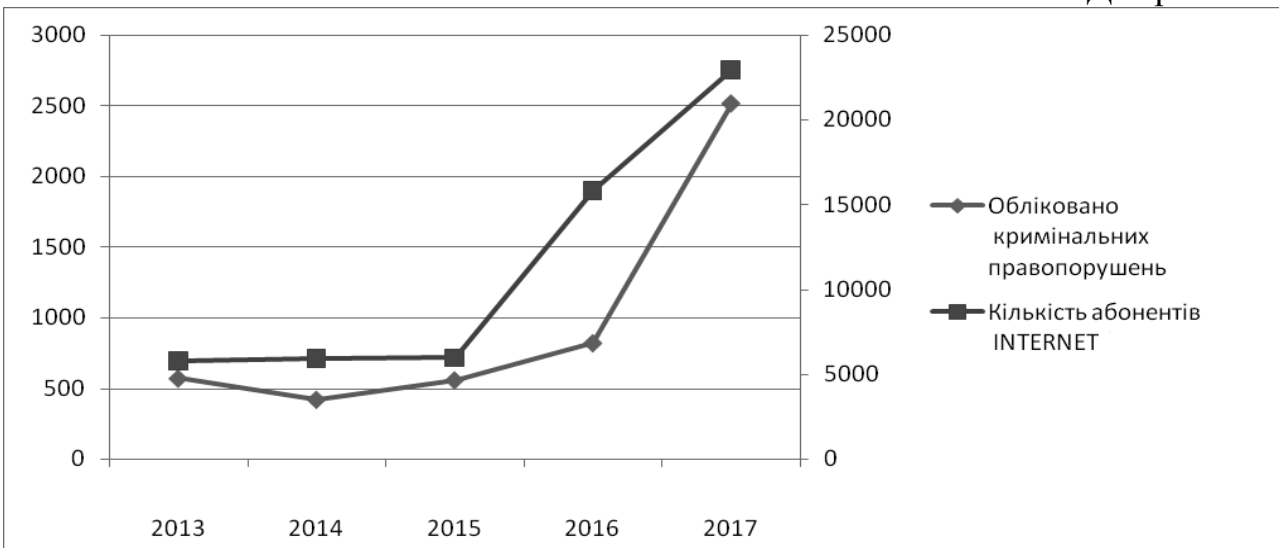
Дослідники зазначають, що одною з потужних детермінантів комп'ютерних злочинів є постійне збільшення кількості пристроїв, які використовують комп'ютерні технології, та їх широке використання в різних сферах суспільного життя. Згідно прогнозу експертів Управління ООН по наркотикам і злочинності у 2020 році кількість пристроїв буде у шість разів перевищувати чисельність населення. За такої ситуації важко уявити комп'ютерний злочин, а можливо, навіть будь-який злочин, який не супроводжувався б електронними доказами, пов'язаними з підключенням до мережі Інтернет [2, p. X].

Порівняльний аналіз облікованих кримінальних правопорушень за даними Генеральної прокуратури України [3] та кількості користувачів мережні Інтернет в Україні за даними Державної служби статистики України [4] засвідчує пряму залежність цих показників (див. Таблиця 1 і Діаграма 1).

Таблиця 1

Період	2013	2014	2015	2016	2017
Обліковано кримінальних правопорушень	568	418	556	818	2514
Кількість абонентів мережі Інтернет	5759,9	5910,8	5951,6	15834,9	22957,5

Діаграма 1



Таким чином можна зробити висновок, що рівень кіберзлочинності буде продовжувати зростати паралельно з рівнем інформатизації суспільства.

Важливою складовою поліпшення протидії кіберзлочинності є поєднання правових методів і методів точних наук під час виявлення та

розслідування кіберзлочинів. Так, зокрема, В. І. Трапезніков наголошує на важливості застосування методу статистичної класифікації кіберзлочинів для організації збору статичних даних про кіберзлочини в рамках інформаційно-аналітичної роботи правоохоронних органів [5, с. 367]. В. В. Мурадов визначає необхідність вдосконалення технічних і правових засад використання електронних доказів в кримінально-процесуальному доказуванні [6]. Передовою у цьому зв'язку є ініціатива MULTI-FORESEE в рамках Європейської співпраці в науці і технологіях (COST), яка вже сьогодні об'єднує зусилля дослідників різних країн світу з метою використання сучасних методів комп'ютерного моделювання, оптики, спектроскопії, хімії, фізики для передачі не лише електронних доказів, а й відбитків пальців, біоречовин, фарби, волокон тощо [7].

Підсумовуючи, зазначимо, що необхідна активізація використання передових цифрових технологій і методів точних наук у протидії кіберзлочинності.

Список використаних джерел:

1. Про основні засади забезпечення кібербезпеки України: закон України від 05.10.2017 р. 2163-VIII. URL: http://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 01.12.2018).
2. Всестороннее исследование проблем киберпреступности, февраль 2013 года. Управление ООН по наркотикам и преступности. URL: https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Russian.pdf (дата звернення: 01.12.2018).
3. Статистична інформація Генеральної прокуратури України за 1913-2018 рр. URL: https://www.gp.gov.ua/ua/statinfo.html (дата звернення: 01.12.2018).
4. Державної служби статистики України URL: http://www.ukrstat.gov.ua.
5. Трапезников В. И. Характеристика и значение международной статистики киберпреступности / В. И. Трапезников // Інформатика та математичні методи в моделюванні. – 2014. – Т. 4, № 4. – С. 363-369.
6. Мурадов В. В. Електронні докази: криміналістичний аспект використання. Порівняльно-аналітичне право. 2013. № 3-2. С. 313-315.
7. Action CA16101 COST Homepage link. URL: https://multiforesee.com/ (дата звернення: 01.12.2018).

УДК 004.056.53

СЕРГІЙ ГЕННАДІЙОВИЧ СЕМЕНОВ
доктор технічних наук, професор, завідувач кафедри обчислювальної техніки та програмування НТУ «ХПІ»
ДЕНИС ГЕННАДІЙОВИЧ ВОЛОШИН
аспірант кафедри обчислювальної техніки та програмування НТУ «ХПІ»

АНАЛІЗ І ПОРІВНЯЛЬНЕ ДОСЛІДЖЕННЯ МЕТОДІВ СТАНУ БЕЗПЕКИ УПРАВЛІННЯ БПЛА В УМОВАХ ВПЛИВУ РАДІОЕЛЕКТРОННОЇ БОРОТЬБИ

Сучасні тенденції розвитку ряду галузей, пов'язаних з геоінформаційними технологіями, вимагають використання недорогих і високоефективних засобів отримання даних. Такими засобами останнім часом стали безпілотні апарати. Як показали дослідження, важко однозначно класифікувати безпілотні літальні апарати (БПЛА) через те, що дані вироби мають дуже різні характеристики (вага, вантажопідйомність, дальність, швидкість, навантаження на крило і т.д.).

Проведені дослідження і аналіз літератури показали, що останнім часом в ряді галузей, наприклад, оборонному відомстві, поліції, пожежних і аварійних службах, все частіше використовуються легкі і надлегкі БПЛА. Пов'язано це багато в чому з необхідністю зменшення ціни і конкуренцією середовища нових постачальників даних апаратів.

У той же час як показали дослідження існує ряд проблем, що знижують ефективність використання БПЛА і погіршують якість розв'язуваних ними завдань. Однією з таких проблем є придушення каналу GPS спеціальними пристроями радіоелектронної боротьби (РЕБ).

Існуючі методи**.**. У БПЛА які літають вище 9-10 км перехоплення сигналу з супутників навігації становить досить важким завданням, крім того, що треба мати дрон здатний літати вище, потрібно зуміти направити його точно над апаратом жертви і супроводжувати його протягом всього перехоплення, до того ж військові канали GPS мають шифрування. Однак БПЛА здатні літати вище 10 км мають велику вартість, їм необхідна злітно-посадкова смуга і фотографування з великої висоти буде негативно позначатися на якості одержуваних даних.

Другий спосіб - це відмова від систем супутникової навігації. Більшість БПЛА мають штатні засоби об'єктивного контролю - відео та фото фіксація. Методи, в основі яких лежить фото / відео фіксації, мають різні підходи до вирішення завдання, проте характеризуються загальними негативними сторонами - високим обчислювальним навантаженням на систему, необхідністю наявності окремої камери для фіксації та аналізу зображень в процесі польоту, високими вимогами до якості одержуваних знімків.

Третій спосіб був розроблений ще в 80-х роках. В його основі лежить інерціальна система позиціонування дрона, яка з певною точність виводить апарату на заданий курс. Після виконання поставленого завдання ця система

повертає його в задану область розміром кілька десятків кілометрів, де вже локальна система позиціонування у вигляді спеціальних радіомаяків направить БПЛА в певну зону.

ВИСНОВКИ

В результаті можна зробити висновок, що жоден з досліджуваних методів не надає всіх необхідних умов для безпечного повернення апарату на позицію старту. Єдиним на сьогодні надійним рішенням для збереження БПЛА в умовах протидії сучасних засобів РЕБ є установка на його борт інерціальної навігаційної системи (ІНС) у сумі зі спеціальними пристроями, які розпізнають втручання в управління апаратом і переводять його у повністю в автономний режим. В цьому випадку навігація здійснюється за рахунок координат, які видаються ІНС, і апарат продовжує виконувати заздалегідь запрограмоване завдання - наприклад, політ по певних точках для ведення розвідки місцевості. Однак точність одержуваних координат від ІНС є досить неточною та потребує істотних доопрацювань.

УДК 343.9

ДМИТРО ЮРІЙОВИЧ УЗЛОВ
канд. техн. наук, начальник Управління інформаційно-аналітичної підтримки ГУНП в Харківській області, полковник поліції
ВОЛОДИМИР МИХАЙЛОВИЧ СТРУКОВ
кан. техн. наук, завідувач кафедри інформаційних технологій факультету № 4 ХНУВС
ОЛЕКСІЙ ВЯЧЕСЛАВОВИЧ ВЛАСОВ
заступник начальника Управління інформаційного-аналітичної підтримки ГУНП в Харківській області, підполковник поліції

МЕТОДОЛОГІЧНИЙ АПАРАТ АНАЛІТИЧНОЇ РОБОТИ В НАЦІОНАЛЬНІЙ ПОЛІЦІЇ

Відповідно до своїх основних повноважень, підрозділи Національної поліції спрямовані на виявлення причин та умов, що сприяють вчиненню кримінальних та адміністративних правопорушень, а також на вжиття у межах своєї компетенції заходів для їх усунення. Реалізація таких заходів стає можливою лише за умови прийняття управлінських рішень на основі використання комплексу методів для збирання, оцінки, аналізу та реалізації інформації при розслідуванні кримінальних правопорушень, а також при розробленні тактичних та стратегічних засад з протидії злочинності.

Відомо, що аналіз і синтез є головними методами мислення. Аналіз (грец. analysis — розкладання, розчленування) і синтез (грец. synthesis — з'єднання, поєднання, складання) — це процеси уявного розчленовування цілого на складові частини і возз'єднання цілого з частин. Поліцейський аналітик виконує саме таку інтелектуальну творчу діяльність, спрямовану на

одержання та використання нових знань, що здійснюється із застосуванням наукових методів та при наявності відповідної форму допуску та доступу до джерел інформації, що міститься у базах (банках) даних Міністерства внутрішніх справ України, Національної поліції України та інших органів державної влади, у т.ч. установ, підприємств, установ та організацій усіх форм власності. Таким чином, аналітик здійснює збір, оцінку, обробку даних з інформаційних ресурсів з метою ідентифікації та якомога більш точному визначенні внутрішніх зв'язків між інформаціями (відомостями, даними), що стосуються кримінальних правопорушень, і будь-якими іншими даними, отриманими з різних джерел, їх використанням в інтересах ведення оперативно-розшукової та слідчої діяльності, їх аналітичної підтримки, а також розроблення тактичних та стратегічних заходів із протидії правопорушенням.

Відповідно до регламенту аналітичної роботи, співробітники поліції все частіше у своїй повсякденній діяльності повинні використовувати сукупності наукових методів з виявлення в похідних даних раніше невідомих, нетривіальних, практично корисних і доступних інтерпретації знань, необхідних для прийняття оптимальних управлінських рішень. Основу таких методів складають всілякі технології класифікації, моделювання і прогнозування, засновані на застосуванні дерев рішень, штучних нейронних мереж, генетичних алгоритмів, еволюційного програмування, асоціативної пам'яті, нечіткої логіки. До них також нерідко відносять статистичні методи (дескриптивний аналіз, кореляційний і регресійний аналіз, факторний аналіз, дисперсійний аналіз, компонентний аналіз, дискримінантний аналіз, аналіз часових рядів, аналіз виживаності, аналіз зв'язків).

Завдання, які вирішуються поліцейськими аналітиками прийнято розділяти на два великі класи: описові та прогностичні. В описових завданнях найголовніше - це дати наочне відображення та опис наявних прихованих закономірностей, в той час як в прогностичних завданнях на першому плані стоїть питання про передбачення для тих випадків, для яких даних ще немає.

До описових завдань відносяться:

пошук асоціативних правил або патернів (зразків);

угруповання об'єктів, кластерний аналіз;

побудова регресійної моделі.

До прогностичних завдань відносяться:

3. класифікація об'єктів (для заздалегідь заданих класів);
4. регресійний аналіз, аналіз часових рядів.

Також слід зазначити, що аналітична робота поліцейського завжди здійснюється на трьох рівнях: оперативному, тактичному та стратегічному:

- при здійсненні оперативного аналізу проводяться дослідження злочинної діяльності підозрюваного, виявлення спільників, потерпілих, встановлення мотивів і цілей вчинення злочинів, встановлення зв'язків між даними, які отримано у процесі розслідування, визначення (підтвердження/спростування) ймовірної рольової участі об'єкта при здійсненні протиправної діяльності, аналіз даних у конкретному провадженні

з метою розділення інформації на елементи, проведення оцінки інформації та аналіз організованої групи;

● при здійсненні тактичного аналізу проводяться розкриття основної спрямованості розвитку злочинності та її окремих видів в минулому, на теперішній час і, як прогноз, у майбутньому, будується система опису криміналістично значущих ознак роду або виду злочинів, аналіз стану злочинності на конкретній території за невеликий проміжок часу, за певним видом злочину чи протиправної діяльності певної групи, проводиться встановлення профілю злочину, встановлення профілю підозрюваного, встановлення профілю потерпілого та аналіз окремих видів злочину;

● при здійсненні стратегічного аналізу проводиться оцінка загроз, спричинених діяльністю організованих злочинних угруповань та скоєних тяжких і особливо тяжких злочинів, здійснюється управління ризиками, що несуть загрозу публічної безпеки і порядку, правам і свободі людини, заходам щодо протидії злочинності, з урахуванням зон ризиків, результатів ідентифікації, верифікації та вивчення учасників злочинної діяльності і закономірностей їх сталого функціонування та складання прогнозів розвитку кримінальних тенденцій при розробці засад протидії злочинності та напрацювання способів їх мінімізації та усунення причин.

УДК 004.89

АНДРІЙ ВОЛОДИМИРОВИЧ СЕРВАТОВСЬКИЙ,
слухач магістратури факультету № 1 Харківського національного університету внутрішніх справ
МИХАЙЛО ЕДУАРДОВИЧ ГЕРАСИМЕНКО,
слухач магістратури факультету № 3 Харківського національного університету внутрішніх справ
ЮРІЙ МИКОЛАЙОВИЧ ОНИЩЕНКО,
кандидат наук з державного управління, доцент, доцент кафедри кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

ПЕРСПЕКТИВИ ВПРОВАДЖЕННЯ ІНТЕЛЕКТУАЛЬНОЇ СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ В УКРАЇНІ

З постійним стрімким розвитком технологій в світі з’являється багато покращених пристроїв та систем відеоспостереження, що застосовуються у різних сферах діяльності сучасного суспільства. Актуальним сьогодні є впровадження відеокамер та інтелектуальних систем відеоспостереження в діяльність поліції для забезпечення публічної безпеки та боротьби зі злочинністю.

Інтелектуальна система відеоспостереження дозволяє контролювати транспортний потік, виявляти правопорушників, розпізнавати, а також звіряти державні номерні знаки, колір і марки автомобілів тощо. Штучний інтелект системи виявляє номерні знаки, встановлені на інше авто, а також

може розпізнати злочинця, який перебуває в розшуку. Якщо раніше необхідно було встановлювати велику кількість моніторів та виводити на них зображення з камер відеоспостереження, а людина повинна була його продивлятись, то наразі система вже автоматично аналізує та видає фрагменти відео, на які необхідно звернути увагу.

Основне завдання інтелектуальної відеокамери – надати можливість функціонально змоделювати зорову систему людини і, в деякій мірі, його мозок, а також інтерпретувати те, що «бачить» камера через штучний розум.

Аналізуючи міжнародний досвід застосування у діяльності поліції інтелектуальних систем відеоспостереження, можна дійти висновку, що вони мають багато переваг:

- якісний збір інформації та її обробка (ідентифікація об’єктів);
- отримання інформації та логічне поєднання відповідностей з відкритих джерел мережі Інтернет, відомчих баз даних та інших інформаційних ресурсів;
- автоматичний режим роботи системи;
- швидкий пошук потрібної інформації про певну подію;
- наявність функції автоматичної аналітики зі сповіщенням оператора системи про певну подію.

У своїй реалізації інтелектуальна система відеоспостереження дозволить працівникам поліції вирішувати наступні завдання:

- розпізнавання облич, у тому числі зі зверненням до розшукових баз даних, забезпечення автоматизованого пропускного режиму;
- розпізнавання автомобільних номерів, типу та моделі автотранспорту, ідентифікація загроз на стратегічно важливих об’єктах;
- автоматичне порівняння з внесеними до існуючих банків даних моделі, кольору та реєстраційного знаку автомобіля та виявлення можливих невідповідностей;
- аналіз траєкторій руху осіб та транспортних засобів, контроль швидкісного режиму руху автомобілів, оцінка та аналіз ситуації на дорогах з метою забезпечення безпеки дорожнього руху, регулювання завантаженості магістралей;
- аналіз інтенсивності транспортних потоків у масштабах міста;
- забезпечення безпеки вокзалів, аеропортів, торгівельних, розважальних та спортивних комплексів, а також інших місць великого скупчення людей шляхом виявлення нетривіальної поведінки;
- виявлення взаємопов’язаних подій та збір відомостей для подальшого проведення тактичного та стратегічного аналізу.

У місті Маріуполі впроваджено інтелектуальну систему відеоспостереження, яка реально функціонує та дає перші результати. Досвід використання інтелектуальної системи відеоспостереження у Маріуполі дозволяє стверджувати, що вона є ефективним інструментом для боротьби зі злочинністю та профілактичним заходом, що позитивно впливає на зменшення динаміки рівня злочинності, дозволяє виявляти та документувати

значно більшу кількість правопорушників, у тому числі тих, хто знаходиться у розшуку, здійснювати ефективний пошук викрадених автомобілів тощо.

Нажаль, запровадження інтелектуальної системи відеоспостереження на всій території України досить проблематично, тому що фінансових можливостей Міністерства внутрішніх справ не вистачить для закупівлі такого коштовного обладнання у достатній кількості. Отже, вбачається цілком допустимим та реальним залучення фінансової підтримки місцевих державних адміністрацій, спонсорів та, навіть, приватного сектору.

УДК 681.518

ДМИТРО ІВАНОВИЧ ЄВСТРАТ
кандидат технічних наук, доцент, доцент кафедри інформаційних технологій факультету № 4 Харківського національного університету внутрішніх справ
ВІКТОРІЯ ЄВГЕНІВНА РОГ
старший викладач кафедри інформаційних технологій факультету № 4 Харківського національного університету внутрішніх справ

ДО ПИТАННЯ ЩОДО ВИБОРУ ТА ОПТИМІЗАЦІЇ СТРУКТУРИ ІНФОРМАЦІЙНОЇ СИСТЕМИ НА ЕТАПІ ЇЇ ПРОЕКТУВАННЯ

Перспективи реалізації проектів багатьох великих систем сьогодні значною мірою залежать від технічних характеристик використовуємої комп'ютерної техніки, функціональних можливостей програмного забезпечення, рівня використання сучасних інформаційно-комунікаційних технологій, здатних вирішувати в реальному масштабі часу складні завдання управління різного роду об'єктами, технологічними і соціально-економічними процесами. Ці завдання відрізняються насиченим функціональним змістом і математичною різноманітністю, високою трудомісткістю, наявністю тенденцій до змін і ускладнення змісту, необхідністю рішення у високому темпі роботи штатного апаратного забезпечення і додаткових технічних пристроїв, що забезпечує високий рівень продуктивності, вимогами до забезпечення оперативності і високої достовірності результатів обчислень, обробки великих масивів даних і перетворення інформації, а також можливістю безперервного рішення впродовж тривалого періоду часу або взагалі, в режимі – 24/7/365. Для вирішення такого класу завдань потрібні інформаційні системи (ІС), в яких надпродуктивність поєднувалася б, як з високою надійністю (в т.ч. стійкістю функціонування програмного забезпечення), якістю і зручністю використання, а також зі здатністю адаптуватися до вимог користувачів, що змінюються. Таким чином, рішення задачі розвитку існуючих, а також розробки принципово нових методологій проектування і побудови сучасних ІС вважається актуальним.

Важливою характеристикою ІС являється їх структура. Визначення поняття структури ІС і її різновиди розглянуті в [1]. Для вирішення завдань

аналізу і синтезу структури ІС використовуються комплекси взаємозв'язаних оптимізаційних, імітаційних і розрахункових моделей. Приклад побудови такого комплексу моделей для вирішення завдання проектування і корекції структури розподілених систем обробки інформації і інших складних систем наведений в [2].

Різноманітність завдань, що вирішуються за допомогою сучасних ІС, привела до появи безлічі різнотипних систем, що відрізняються складом і характером взаємодії підсистем, принципами побудови, правилами обробки інформації. При цьому, існує значна кількість методологій проектування ІС, залежних від їх типу. Розглянемо коротко деякі з них.

Організація *канонічного проектування ІС* орієнтована на використання головним чином каскадної моделі життєвого циклу ІС. Типова методологія побудови ІС систем містить три основні компоненти:

- набір типів моделей (як правило це моделі структурного і об'єктного підходів) для опису вимог до ІС, проектних і програмних рішень;
- методика застосування набору моделей для побудови ІС;
- процес організації проектних робіт.

Метод функціонального моделювання що використовується при цьому дозволяє оптимізувати існуючі процеси, з метою подальшої автоматизації їх виконання, проте для оптимізації конкретних технологічних операцій функціональної моделі може бути недостатньо. В цьому випадку доцільно використати *імітаційне моделювання*. Такий підхід дозволяє врахувати в імітаційній моделі час виконання операцій, забезпечує якнайповніший аналіз динаміки процесів, а сама імітаційна модель описує не лише потоки сутностей, інформації і управління, але і різні метрики. Отриману модель можна "програти" в часі і отримати статистику процесів, що відбуваються, так, як це було б в реальності. У імітаційній моделі зміни процесів і даних асоціюються з подіями, а "програвання" моделі полягає в послідовному переході від однієї події до іншої.

Типове *проектування ІС* припускає створення системи з готових типових елементів. Основополагаючою вимогою для застосування методів типового проектування є можливість декомпозиції проектованої ІС на безліч складових компонентів (підсистем, комплексів завдань, програмних модулів і так далі). Для реалізації виділених компонентів вибираються наявні на ринку типові проектні рішення, які настроюються відповідно до вимог системи, що розробляється.

Однією з основних частин інформаційного забезпечення ІС є інформаційна база. Для її розробки виконується моделювання даних (найбільш поширеним засобом *моделювання даних* є діаграми "суть-зв'язок" (ERD).), а у разі використання сховищ даних і виконання в ІС аналітичних запитів, що забезпечують підтримку ухвалення рішень – здійснюється *проектування сховищ даних*.

Розглянуті методології проектування ІС забезпечують структуризацію інформаційного простору як об'єкту автоматизації з метою забезпечення функціональних вимог, як до самої ІС, так і до характеристик процесу її

розробки, зниження складності процесу створення ІС, підвищення якості постановки завдання, застосування сучасних методів і технологій створення ІС на усьому її життєвому циклі. Вибір і оптимізація структури ІС на етапі її проектування дозволяють спростити рішення таких завдань, як:

- розробка і модернізація ІС (за рахунок спеціалізації груп проектувальників підсистем);
- впровадження і постачання готових підсистем відповідно до черговості виконання робіт;
- експлуатація ІС (внаслідок спеціалізації працівників предметної області).

Список використаних джерел:

1. Шастова Г.А., Коекин А.И. Выбор и оптимизация структуры информационных систем. – М.: Энергия, 1972. – 256 с.

2. Габалин А.В. Вопросы оптимизации структуры распределенных систем обработки информации // Прикладная информатика. 2007. Т. 6. С. 129-136.

УДК 004.02 - 65.012.2

ИГОРЬ ГЕНРИХОВИЧ ИЛЬГЕ
кандидат технических наук, доцент, доцент кафедры автоматизации и компьютерно-интегрированных технологий Харьковского национального автомобильно-дорожного университета

МОДЕЛЬ ВЫБОРА ПРОГРАММНЫХ СРЕДСТВ УПРАВЛЕНИЯ ПРОЕКТАМИ ПОДГОТОВКИ КАДРОВ НПУ

Разработка современных проектов подготовки кадров является сложным и трудоемким процессом, протекающим в условиях нечеткой информации и жестких ограничений по времени разработки и по доступным ресурсам. Это обуславливает необходимость использования программных систем управления проектами, причем их выбор в значительной степени определяет эффективность планирования и ведения проекта. Поэтому актуальна задача разработки модели выбора программных средств для управления проектов подготовки кадров НПУ с учетом нечеткой информации.

Модель выбора программных средств для комплексной автоматизации ведения работ в проектной организации основывается на теории нечетких множеств [1; 2].

Выбор программного продукта для управления проектами организации будем проводить на основе анализа программных средств – лидеров этого сегмента рынка программного обеспечения, а именно Microsoft Project Professional, Primavera P3e, Spider Project, Open Plan.

Сопоставление этих продуктов проводится по четырем группам критериев [3], а именно по возможности планирования проекта, по средствам

отслеживания и управления проектом, по поддержке коллективной работы и по оценке применимости.

Возможности планирования проекта оцениваются по следующим критериям:

- доступность интерфейса и наличие интерактивных самоучителей;
- трудоемкость разработки структур работ с учетом связей;
- трудоемкость разработки структур ресурсов с учетом наличия мастеров;
- управление пулами ресурсов проектного подразделения;
- управление портфелями проектов;
- средства оптимизация планов проекта;
- оценка влияния рисков.

Средства отслеживания и управления проектом оцениваются по:

- возможности план/фактного анализа;
- средства формирования запросов и отчетов о статусе работ;
- оценка освоенного объема;
- работа на основе промышленной СУБД (SQL Server);
- проектная статистика на базе промышленного OLAP-сервера.

Критериями для оценки коллективной работы являются:

- Web-доступ к проектной информации;
- Web-анализ состояния ресурсов;
- поддержка мобильных средств;
- взаимодействие с исполнителями;
- средства для информирования высшего управленческого звена и принятия стратегических решений;
- интегрированная поддержка проектного документооборота.

Для оценки применимости критериями являются:

- оптимальное сочетание цена/качество;
- сеть внедрения;
- консалтинговая поддержка.

Полагаем, что перечисленные выше критерии равно важны. Множество альтернатив Z при выборе состоит из четырех программных продуктов, обозначаемых z_i:

$$Z = \{z_1, z_2, z_3, z_4\} \quad (1)$$

где z_1- MS Project Professional, z_2 - Primavera P3e, z_3- Spider Project, z_4- Open Plan.

Для оценки альтернатив используем множество из 22-х равнозначных критериев:

$$K = \{K_i\}, i = 1,22 \quad (2)$$

где $\{K_i\}$,- перечисленные выше критерии.

Оценки альтернатив по каждому из вышеприведенных критериев $\{K_i\}$ можно представить в виде нечеткого множества:

$$A(K_i) = (\nu_{K_i}(z_1), \nu_{K_i}(z_2), \nu_{K_i}(z_3), \nu_{K_i}(z_4)\ ) \quad (3)$$

где $\nu_{K_i}(z_l)$ - оценка альтернативы $z_l\ (l = \overline{1,4})$ по критерию $K_i\ (i = 1,22)$

Альтернатива z_l, которая в наибольшей степени соответствует требованиям всей совокупности критериев, принимается в качестве решения задачи выбора.

Для выбора наилучшей альтернативы считаем, что решающее правило R лежит на пересечении соответствующих нечетких множеств:

$$R = A(K_1) \cap A(K_2) \cap A(K_3) ... \cap A(K_i) \quad (4)$$

Функция принадлежности искомого решения в соответствии с определением операции пересечения нечетких множеств может быть определена зависимостью

$$\nu_R(z_l) = \min_{i=1,n} (\nu_{A(K_i)}(z_l)), l = \overline{1,4} \quad (5)$$

Альтернатива $z^{\#}$, для которой значение функции принадлежности $\nu_R(z_l)$ окажется максимальным, будет наилучшей, т.е.

$$\nu_R(z_l^{\#}) = \max_{l=1,4}(\nu_R(z_l)) \quad (6)$$

Альтернатива $z^{\#}$ в наибольшей степени удовлетворяет всем критериям в совокупности и является решением поставленной задачи выбора программного продукта для управления проектами.

Таким образом, в работе построена модель выбора программных средств для управления проектов подготовки кадров НПУ, которая в отличии от существующих позволяет учитывать нечеткость информации.

СПИСОК ИСПОЛЬЗОВАНЫХ ИСТОЧНИКОВ

1. Пономарев, А. С. Нечеткие множества в задачах автоматизированного управления и принятия решений: учебное пособие [Текст] / А. С. Пономарев. – Харьков: НТУ ХПИ, 2005. – 232 с.

2. Методы и модели принятия решений в условиях многокритериальности и неопределенности: монография [Текст] / [Э. Г. Петров, Н. А. Брынза, Л. В. Колесник, О. А. Писклакова] ; под.ред. Э. Г. Петрова. – Херсон: Гринь Д.С., 2014. – 192 с.

3. Материалы по сравнению и обзору Open Plan Professional, Primavera, Microsoft Project, Spider Project [Электронный ресурс]. - Режим доступа: http://ivn73.tripod.com/ MS_Project_Primavera_Open_Plan.htm

УДК 004[681.518]

ДМИТРО ВІКТОРОВИЧ СПАСІБОВ
кандидат технічних наук, начальник відділу технічного захисту інформації Департаменту інформаційно-комп'ютерного забезпечення Харківської міської ради, аспірант кафедри інформаційних технологій і систем управління ХарРІ НАДУ

ОБҐРУНТУВАННЯ МЕХАНІЗМІВ ТРАНСКОРДОННОЇ Е-ВЗАЄМОДІЇ ОРГАНІВ ПОЛІЦІЇ В ПУБЛІЧНОЇ СФЕРІ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЕФЕКТИВНОГО УПРАВЛІННЯ

Механізми е-взаємодії забезпечують інформаційну взаємодію органів поліції в е-формі під час доступу до інформаційних баз, реєстрів, надання е-послуг та виконання державних функцій (рис. 1).

Рис. 1. Класифікація механізмів е-взаємодії

Результатом е-взаємодії може бути отримання інформації, надання консультації або прийняття управлінського рішення. Відповідно з цим за результатом взаємодії можна класифікувати процедури е-взаємодії на інформаційні, консультативні та прийняття рішень.

Інформаційні механізми забезпечують отримання необхідних даних за допомогою сервісних інструментів доступу до інформаційних реєстрів, кадастрів, інформаційних даних як загального так і спеціального призначення.

Механізми консультування передбачають обов'язкову наявність запиту з боку можливого одержувача послуг і наявність обов'язкової відповіді з боку суб'єкта надання послуги в довільній формі або у формі документа. Процедури консультування забезпечують не тільки більш відкрити органи поліції, але й урахування думок користувачів. Для цього публікується кодекс практики консультування, у якому є положення про налагодження механізмів зворотного зв'язку.

Механізми прийняття рішень забезпечують урахування та використання пропозицій громадян у діяльності поліції. Е-урядування розвинених країн світу інтегровано в мережеву інформаційно-комунікаційну інфраструктуру, що виходить за жорсткі організаційні рамки органів поліції та підключає до себе ресурси мережевої громадськості, що забезпечують

ефективну репрезентацію групових інтересів і вплив індивідуальних, колективних та організаційних цивільних структур на розроблення правоохоронних рішень.

Механізми е-взаємодії за рівнем взаємодії можна класифікувати на односторонні, інтерактивні та трансакційні.

Односторонні механізми е-взаємодії передбачають: інформування громадськості про діяльність органів поліції; надання нормативно-правового забезпечення про діяльність органів влади; оперативне публікування офіційних джерел; відкриття доступу до публічної інформації та відкритих даних; формування звітних е-форм та надання допомоги з правил їхнього оформлення тощо.

Реалізація цих механізмів досягається за допомогою офіційних сайтів та порталів органів поліції, інформресурсів соціальних мереж, блогів, відеоконференцій, е-засобів доставки новин, списків розсилок, інтермедії, мобільної телефонії. Процес інформування не передбачає інтерактивних дій з боку одержувача е-послуг або надання ним яких-небудь документів.

Інтерактивний (двостороння) механізм е-взаємодії забезпечує двосторонню взаємодію влади з суспільством за допомогою е-комунікацій. У процесі інтерактивної взаємодії користувач має змогу звернутися з конкретним запитом, і він може отримати конкретну відповідь державних структур щодо своєї проблеми [1].

Трансакційні механізми е-взаємодії передбачають доступ конкретним фізичним або юридичним особам тільки після того, як вони задовольняють відповідним вимогам з точки зору їхніх ідентифікації та автентифікації та подальшого здійснення реальних операцій (трансакцій) з надання е-послуги. Трансакційними послугами неможливо скористатися без попередньої аутентифікації, оскільки надання послуги пов’язано з обробленням індивідуальної та унікальної інформації [1].

Таким чином, механізми е-взаємодії забезпечують інформаційну взаємодію органів поліції в е-формі під час надання е-послуг та виконання державних функцій. Результатом е-взаємодії може бути отримання інформації, надання консультації або прийняття управлінського рішення. Відповідно, за результатом взаємодії можна класифікувати механізми е-взаємодії на інформаційні, консультативні та прийняття рішень. Механізми е-взаємодії за рівнем взаємодії можна класифікувати на односторонні, інтерактивні та трансакційні.

У зв'язку з розвитком світових інтеграційних процесів найперспективнішим напрямом, покликаним задовольнити ці процесі, є забезпечення захищеної транскордонної е-взаємодії. Серед основних проблем забезпечення такої взаємодії є розроблення ефективного і надійного механізму управління правами суб'єктів. Одним із шляхів підвищення ефективності механізму управління правами є організація транскордонної інфраструктури управління правами на базі уповноважених операторів. Однак управління правами при е-взаємодії проблематичне щодо прав, володіння якими реалізується через володіння документом. Другим із

підходів до управління правами є підхід, заснований на застосуванні технології інфраструктури відкритих ключів. При цьому правомочність суб'єкта вказується в його атрибутивному сертифікаті [2].

Технологія атрибутивних сертифікатів здається тим рішенням, яке дозволяє максимально ефективно вирішувати всі завдання управління правами суб'єктів у транскордонному просторі. При цьому інфраструктура управління правами може будуватися на базі широко застосованої інфраструктури відкритих ключів, що добре себе зарекомендувала.

Список використаних джерел:

1. Клімушин П. С. Стратегії та механізми електронного урядування в інформаційному суспільстві. Монографія. Харків. Вид-во ХарРІ НАДУ «Магістр», 2016. 524с.

2. Сазонов А. В. Инфраструктура и технология управления правами субъектов в трансграничном пространстве. Вопросы защиты информации. – 2012. № 3. С. 83–87.

УДК 004.02 - 65.012.2

ОЛЕНА ГЕОРГІЇВНА СОКОЛОВСЬКА
кандидат технічних наук, доцент, доцент кафедри інформаційних технологій ХНУВД
ІГОР АНДРІЙОВИЧ ЧУБ
доктор технічних наук, професор, начальник кафедри пожежної профілактики в населених пунктах Національного університету цивільного захисту України

ОПТИМІЗАЦІЯ РОЗМІЩЕННЯ ПІДРОЗДІЛІВ НПУ В МІСТІ

Пропонується нова методика визначення оперативної дислокації сил НПУ і наводяться алгоритми для її програмної реалізації. В основі запропонованої методики лежить наступний підхід.

Територія розбивається на ділянки, які включають в себе довколишні об'єкти, що патрулюються. Число ділянок відповідає кількості нарядів НПУ. Отримані ділянки повинні містити таке число об'єктів, що б їх сумарні коефіцієнти криміногенності були однакові. Під коефіцієнтом криміногенності об'єкта розуміється кількість правопорушень і злочинів, скоєних за проміжок часу або сукупність проміжків часу. Таким чином, ділянки території, де відбувається більше злочинів та інших правопорушень, включають в себе менше об'єктів і перекриваються маршрутами меншої довжини. Далі на кожному отриманому ділянці розробляється оптимальний маршрут обходу об'єктів, що патрулюються.

Запропонована типова методика розстановки сил НПУ є дворівневою ієрархічною системою. На вищому рівні проводиться формування ділянок з урахуванням двох критеріїв:

• мінімізації відстані між об'єктами, що входять в одну ділянку;

• рівномірність навантаження нарядів НПУ на ділянках з урахуванням коефіцієнтів криміногенності.

На нижчому рівні розраховуються оптимальні по довжині маршрути обходу всередині кожної ділянки.

Розглянемо математичну постановку задачі верхнього рівня. Для цього представимо територію як множину криміногенних об'єктів з їх координатами, нумерація приймається довільно. Введемо наступні позначення: i - номер об’єкта; S – назва об’єкта; m - число об’єктів; x_i, y_i - координати об’єкта; λ_i - коефіцієнт криминогенности i-го об’єкта; j - номер ділянки, закріпленої за одним нарядом НПУ; n_1 - кількість нарядів; ρ_{ij} - евклідова відстань від i-ого об’єкта до центра j-ої ділянки.

Під центром ділянки розуміємо точку с координатами

$$x_i = \frac{\sum_i x_i \lambda_{ij}}{\sum_i \lambda_{ij}},$$

$\lambda_{ij} \in \{0,1\}$ - символ включення i-ого об’єкта в j-у ділянку;

В якості критеріїв задачі цього рівня використовуємо:

1) компактність ділянок

$$\sum_i \rho_{ij} \to \min, \quad j = \overline{1,n} \tag{1}$$

2) рівномірність навантаження на наряди НПУ

$$\left| \sum \alpha_i \lambda_{ij} - \frac{1}{n} \sum_i \alpha_i \right| \to \min, \quad j = \overline{1,n} \tag{2}$$

Для розв'язання задачі пропонується евристичний алгоритм, який дозволяє знайти, якщо не оптимальний, то досить близький до нього розв’язок.

Сутність алгоритму полягає в наступному:

1) На початку приймається кількість ділянок n_1 рівною кількості об'єктів m і далі вони зменшується ітераційним шляхом. В кінці роботи алгоритму має бути $n_1 = n$ при виконанні зазначених критеріїв.

2) На кожному наступному кроці до будь-якої ділянкі приєднується один об'єкт, обраний за критерієм

$$\min_i S_{ij} = \min_j S_{ij} \qquad \left(i = \overline{1,m}, j = \overline{1,n_1}\right).$$

Це відбувається до тих пір, поки кількість ділянок не стане рівною кількості нарядів НПУ $n_1 = n$.

Після виконання алгоритму кожен з об'єктів включається в яку-небудь ділянку за критерієм близькості, проте при цьому не враховується ступінь

криміногенності об'єктів. Тому для виконання критерію (2) будемо здійснювати перенесення об'єктів з ділянки в ділянку з метою його досягнення. Перенесення здійснюється за допомогою множини однотипних кроків, на кожному з яких визначається ділянка V_k з мінімальним рівнем сумарної криміногенності

$$K : V_k = \min_j \sum_i \alpha_i \lambda_{ij} .$$

Далі для k-ї ділянки визначається об'єкт, що належить до будь-якої з інших ділянок ($\lambda_{ik} = 0$), для якого досягається

$$\min_i \rho_{ik} \lambda_{i, j \neq k} .$$

Потім цей об'єкт переноситься з j-ої ділянки д k-ої. Процедура повторюється до тих пір, поки ступінь нерівномірності сумарного коефіцієнта криміногенності нарядів НПУ не досягне прийнятного рівня ε:

$$\left| \sum_i \alpha_i \lambda_{ij} - \frac{1}{n} \sum_i \alpha_i \right| \leq \varepsilon$$

Оптимізаційна задача, яка розв'язується на нижчому рівні ієрархії, зводиться до відомої задачі комівояжера: необхідно знайти мінімальний (найкоротший) шлях обходу всіх об'єктів, включених в j-у дільницю, тобто побудувати найкоротший цикл.

Ця задача розв'язується для кожної j-ої ділянки. Математична постановка задачі наступна:

$$\sum_i \sum_k \rho_{ik} x_{ik} \rightarrow \min , \quad \sum_i x_{ik} = 1 , \quad \sum_k x_{ik} = 1 \quad \text{для усіх об'єктів,}$$

$$x_{ik} = \begin{cases} 1, & \text{якщо цикл містить перехід з } i \text{ - го об'єкта до } k \text{ - го} \\ 0, & \text{в іншому випадку} \end{cases}$$

УДК 004.912:004.8
ОЛЕКСІЙ ФЕЛІКСОВИЧ ЛАНОВИЙ
кандидат технічних наук, доцент, доцент кафедри програмної інженерії Харківського національного університету радіоелектроніки
ОЛЕГ ВІКТОРОВИЧ ЗОЛОТУХІН
кандидат технічних наук, доцент, доцент кафедри штучного інтелекту Харківського національного університету радіоелектроніки

ЗАСТОСУВАННЯ НЕЙРОМЕРЕЖЕНОГО ПІДХОДУ ДЛЯ КЛАСИФІКАЦІЇ ВТРУЧАНЬ В РОБОТУ КОМП'ЮТЕРНИХ СИСТЕМ

Розглянуто задачу класифікації в комп'ютерних системах на основі нечіткої імовірнісної нейронної мережі в режимі реального часу.

Комп'ютерна система – інформаційно-технічний комплекс, метою якого є обробка, збереження, введення-виведення інформації. До складу комп'ютерної системи входять комп'ютери, принтери, сервери тощо, а також власне програмне забезпечення. Через комп'ютерну мережу з використанням локальних або глобальних протоколів передачі даних здійснюється обмін інформацією. Для опису систем використовують технічні, організаційні, документальні, функціональні, алгоритмічні, програмні та інформаційні структури. Задачі, які розв'язуються в комп'ютерних інформаційних системах, мають ряд характерних особливостей, що впливають на технологію автоматизації обробки даних. Комп'ютерна система дозволяє здійснювати інтеграцію з іншими інженерними технологіями, розширювати можливості й створювати єдине середовище. Саме у такому середовищі може зберігатися інформація про результати несанкціонованого втручання в роботу комп'ютерних систем у вигляді логів, журналів, тонких слідів тощо, що містять базові ознаки текстових даних.

У масиві текстових даних може бути виділено різну кількість класів, до яких вони можуть відноситися. При цьому передбачається що дані класи можуть мати в n-вимірному просторі різну форму і взаємно перекриватися. Архітектура багатошарової адаптивної нечіткої імовірнісної нейронної мережі дозволяє вирішувати задачу класифікації в послідовному режимі по мірі надходження нових даних. Відповідно до реалізації програмної системи розроблено алгоритм навчання багатошарової адаптивної нечіткої імовірнісної нейронної мережі, а також вирішена задача класифікації на основі запропонованої архітектури в умовах пересічних класів, що дозволяє відносити один екземпляр текстового документа до різних класів з різним ступенем імовірності. Архітектура нейронної мережі, що забезпечує виконання класифікації за обраними ознаками, відрізняється простотою чисельної реалізацією і високою швидкістю навчання. Вона призначена для обробки великих масивів даних, що характеризуються векторами ознак високої розмірності. Пропонована нейронна мережа та метод її навчання призначені для роботи в умовах пересічних класів, що відрізняються як формою, так і розмірами.

На сьогоднішній день класифікація інформації в комп'ютерних системах вважається досить складною проблемою. Класифікація є діяльністю, яка стає все більш значимою у зв'язку з постійним зростанням та величезним обсягом доступної інформації і проблемою пошуку інформації. Крім того, значна кількість баз даних є політематичною з великою кількістю категорій, які ускладнюють розв'язання задачі класифікації тексту. Виникли нові проблеми, серед яких найбільш гострою є інформаційна перевантаженість і, як наслідок, необхідність класифікації послідовності документів, які надходять до систем збереження інформації в режимі реального часу. On-line класифікація такого типу текстових документів є нетривіальним завданням, оскільки в невеликому фрагменті тексту може міститися дуже цінна інформація, і віднесення до відповідного класу не можна ігнорувати, а близько розташовані класи можуть перетинатися і/або зливатися. Тому бажано врахувати належність аналізованого документа до кожного з потенційно цікавих для користувача класів. У той же час більшість відомих методів класифікації відносять текстовий документ до одного з чітко помітних класів. Відсутність можливості отримати найбільш актуальну і повну інформацію по конкретній темі втрачає своє значення більшу частину накопичених ресурсів. Оскільки дослідження конкретного завдання вимагає все більших трудовитрат на безпосередній пошук і аналіз інформації по темі, багато рішень приймаються на основі неповного подання про проблему.

Запропонований авторами нейромережевий підхід для класифікації втручань в роботу комп'ютерних систем на підставі аналізу журналів дозволяє вирішувати задачу з точки зору як нечіткої, так і ймовірнісної класифікації, що забезпечує їй перевагу в порівнянні з класичними Байєсовими мережами й імовірнісними нейронними мережами, всі з яких не можуть вирішувати завдання в умовах перекриваються класів. Стає можливим визначити більш точні значення ймовірностей приналежності вхідного текстового об'єкта до кожного з потенційно можливих класів. Даний метод передбачає можливість обробки інформації по мірі її надходження, характеризується простотою реалізації і високою швидкістю обробки інформації.

Висновки

Розглянуто задачу одночасної on-line нечіткої та ймовірнісної класифікації в комп'ютерних системах, що надходять на обробку послідовно в реальному часі. Введена архітектура нейронної мережі, яка класифікує, відрізняється простотою чисельної реалізації та високою швидкістю навчання і призначена для обробки великих масивів даних, що характеризуються векторами ознак високої розмірності. Пропонована нейронна мережа і метод її навчання призначені для роботи в умовах пересічних класів, що відрізняються як формою, так і розмірами.

УДК 311
СВІТЛАНА МИКОЛАЇВНА ВИГАНЯЙЛО
кандидат економічних наук, доцент кафедри соціально-економічних дисциплін Сумської філії Харківського національного університету внутрішніх справ

ОСОБЛИВОСТІ ВИКЛАДАННЯ ПРАВОВОЇ СТАТИСТИКИ ПРИ ПІДГОТОВЦІ КАДРІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Основною причиною відриву правової науки від практики були недостатнє використання, закритість та недоступність даних правової, а точніше кримінально-правової, адміністративно-правової та цивільно-правової статистик.

При підготовці кадрів для інформаційно-аналітичних підрозділів Національної поліції України особливе місце відводиться дисципліні Правова статистика. Вивчення правової статистики має особливе значення при підготовці висококваліфікованих фахівців в галузі юриспруденції, оскільки для науково обґрунтованого пізнання тенденцій і закономірностей розвитку суспільного життя, в тому числі правових явищ, обов'язково мати навички їх аналізу.

При проведенні кримінологічних досліджень інформаційно-аналітичний працівник повинен здійснювати всебічний аналіз діяльності правоохоронних органів, виявляти детермінанти, стан, структуру та тенденції зміни злочинності.

При вивченні дисципліни особливу увагу слід приділити новим підходам до методології статистичної науки. Статистична методологія ґрунтується на загально-філософських і загальнонаукових принципах, на поєднанні аналізу і синтезу.

Методи застосовуються для збирання, оброблення та аналізу статистичної інформації. При вивченні дисципліни в статистиці на базі загальних принципів діалектичного методу розроблені такі специфічні методи:

Метод масового статистичного спостереження (науково організоване збирання та реєстрація фактів та явищ суспільного життя).

Метод зведення та групування виявляє у суспільному явищі найважливіші типи, характерні групи та підгрупи за ознаками.

Метод відносних величин використовується для характеристики кількісного співвідношення різних суспільних явищ.

Метод середніх величин дозволяє охарактеризувати типовий розмір ознаки сукупності в конкретних умовах простору і часу.

Табличний та графічний методи як способи наочного подання наслідків статистичного дослідження.

Індексний метод надає можливість охарактеризувати зміну рівня суспільного явища в часі та просторі, або у порівнянні з запланованим завданням, нормою чи стандартом.

Кореляційний метод виявляє щільність взаємозв'язку явищ суспільного життя.

Статистичний аналіз зведених даних та опрацьованого матеріалу виявляє закономірності та зв'язки суспільних явищ (варіація, інтенсивність розвитку, узагальнюючі індекси).

Також досить активно в статистичних дослідженнях застосовуються математичні методи. Адже статистика досліджує характеристики суспільних явищ, визначає їх кількісне вираження. Математика та статистика використовують спільні методи обробки та оцінки даних, але різні предмети пізнання.

Всі ці методи важливі і широко застосовуються на різних етапах статистичного дослідження.

Будь-яке статистичне дослідження послідовно проходить три етапи. Підготовча частина включає до себе вивчення проблеми дослідження, розробку напрямків, визначення понятійного апарату та питання методологічного і матеріально-технічного забезпечення дослідження.

На першому етапі проходить збір первинного матеріалу (реєстрація фактів, опитування респондентів). На другому етапі зібрані дані підлягають систематизації та групуванню. Третій етап передбачає аналіз варіації, динаміки, взаємозалежностей. За результатами аналізу описуються висновки у формі тексту чи табличній формі або у вигляді графіків.

В результаті вивчення навчальної дисципліни «Правова статистика» здобувач вищої освіти повинен вміти застосовувати статистичні методи; формувати план статистичного спостереження; збирати та фіксувати первинні статистичні дані; виявляти помилки спостереження та контролювати вірогідність даних; виконувати статистичне групування та зведення; проводити узагальнення і аналіз даних; використовувати статистичну методологію для побудови рядів варіації та розрахунку показників варіації правових явищ; аналізувати динаміку правових явищ, застосовувати ряди динаміки при дослідженні тенденцій злочинності; розраховувати показники рядів динаміки; визначати тенденції розвитку явищ та процесів в динаміці; проводити прогностичні розрахунки показників динаміки; різними способами планувати вибіркове спостереження та оцінювати помилку вибірки; здійснювати кореляційний аналіз; використовувати індексний метод; застосовувати рейтинговий метод для аналізу результатів роботи правоохоронних підрозділів.

Список використаних джерел

1. Камлик М.І. Правова статистика. Навчальний посібник. К: Атіка, 2004.-240 с.
2. Правова статистика: [навчальний посібник] / [М.П. Пихтін, Г.С. Поліщук, М.І. Шерман та ін.]; за заг. ред. М.П. Пихтіна.- К.: ФОП О.С. Ліпкана, 2011.-272 с.

УДК 004.04
ЯНА ОЗЕРЯНСЬКА
студентка спеціальності «Право»
Сумської філії Харківського національного університету внутрішніх справ
ІРИНА ОМЕЛЬЧЕНКО
студентка спеціальності «Право»
Сумської філії Харківського національного університету внутрішніх справ
СВІТЛАНА МИКОЛАЇВНА ВИГАНЯЙЛО
кандидат економічних наук, доцент кафедри соціально-економічних дисциплін Сумської філії Харківського національного університету внутрішніх справ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ

Для результативної праці правоохоронних органів в умовах сьогодення є обов'язкове використання інформаційних технологій у ході розслідування та розкриття злочинів. Це обумовлено перш за все тим, що обробляється досить великий обсяг статистичної, аналітичної та поточної інформації.

Важливим завданням юридичної освіти у вищих навчальних закладах системи МВС є надання здобувачам знань та досвіду використання інформаційних технологій, які використовуватимуться в практичній діяльності правоохоронних органів.

Актуальною є проблема використання інформаційних технологій в роботі правоохоронних органів, та підвищення рівня володіння технологіями випускниками ВНЗ системи МВС. Даним проблемам присвячені роботи зарубіжних і вітчизняних дослідників С. Я. Казанцева, Г. В. Єпура, М. І. Ануфрієва, О. М. Бандурки та ін. Але недостатньо з'ясованим залишається питання оволодівання здобувачами сучасного програмно-апаратного забезпечення професійної діяльності працівників міліції [1].

Завдання та методи дослідження. В результаті досліджень було виявлено: різноманітність програмно-апаратного забезпечення професійної діяльності працівників МВС, що використовуються для накопичення інформації; різноманітність інформаційних систем та інформаційних технологій, якими працівники правоохоронних органів користується у своїй діяльності; дослідили обсяг і складність інформаційного забезпечення робочого місця кожного співробітника правоохоронних органів; виявили важливість утворення професійної інформаційної обізнаності курсантів у ВНЗ системи МВС [2].

Чималий об'єм інформації потребує не лише накопичення, але й аналітичної обробки, що полягає у кваліфікованому відборі та систематизації. Керування оперативною інформацією складається з декількох підрозділів: інформаційно-довідкове відділення, відділ кримінальної інформації, відділ оперативно-довідкових обліків, відділ статистики, архівний підрозділ та комп'ютерний центр.

Головною задачею комп'ютерного центру є розробка та впровадження в практичну роботу підрозділів ОВС нових інформаційних технологій та гарантування безпеки даних в системах і мережах.

На нашу думку підвищити ефективність керування оперативною інформацією допомагає використання цілого ряду автоматизованих інформаційних систем, до яких належить оперативно-довідкова, адміністративна, оперативно-розшукова та статистична.

Співробітник кожного підрозділу ОВС у власній роботі використовує спеціальні програми та автоматизовані робочі місця.

Цей огляд виконано з однією метою - продемонструвати обсяг та складність інформаційного забезпечення роботи будь-якого службовця правоохоронних органів. Отже, щоб виконувати свої функціональні обов'язки на належному рівні, службовець правоохоронних органів повинен мати досить високий рівень інформаційної компетентності. Через те, одним із найважливіших завдань професійної підготовки курсантів у ВНЗ системи МВС є формування їхньої професійної інформаційної компетентності.

Підсумовуючи вище сказане можна зробити висновок, що одним з найважливіших способів формування інформаційної компетентності вищих навчальних закладів системи МВС України має стати опановування теоретичних засад утворення, користування і надзвичайно практичного застосування способів програмно-технічного забезпечення професійної діяльності службовців ОВС, що послуговуються в їх практичній діяльності. З цією метою доречно на базі вищого навчального закладу організувати локальну інформаційну мережу, яка б надавала доступ до дієвого Інтегрованого банку даних УМВСУ. Якщо, інформаційна система має інформацію з обмеженим доступом, разом з керуванням оперативної інформації УМВС області винайти тренажери (моделі, навчальні варіанти) цих автоматизованих інформаційних систем. Ці системи можна використовувати кафедрами інформаційних технологій, спеціальних кафедр (ОРД, кримінального права, кримінального процесу, криміналістики, адміністративного права) та при вивченні дисципліни "Інформаційні забезпечення професійної діяльності".

У правоохоронних органах проводяться роботи щодо впровадження нових інформаційних технологій, проектування та побудови нових інформаційних мереж, запровадження нових підсистеми. Саме цей фактор спонукає до подальших наукових досліджень спільно з професіоналами підрозділів МВС. Розробляються і запроваджуються в навчальну та практичну діяльність правоохоронних органів загальні науково-практичні рекомендації, навчально-методичне забезпечення та передовий досвід застосування інформаційних технологій у професійній інформаційній діяльності працівників поліції.

Список використаних джерел

1. Матеріали сайтів http://www.compulog.ru/komit/infores, http://www.insoft.ru/insoft/gibdd, http://www.kmu.gov.ua/, http://www.ncjrs.org/, http://www.ojp.usdoj.gov/cmrc.

2. Саницький В. А. та ін. Система інформаційного забезпечення ОВС України: Навч.-практ. посібник. — К.: Редакційно-видавничий відділ МВС України, ТОВ «АНЕТКС», 2000. — 144 с.

УДК 623.746+351.74

ВЛАДИСЛАВА РУСЛАНІВНА ПОПОВА
курсант 1 курсу факультету № 4 Харківського національного університету внутрішніх справ
ОЛЕКСІЙ МИХАЙЛОВИЧ РВАЧОВ
старший викладач кафедри кібербезпеки факультету № 4
Харківського національного університету внутрішніх справ

НАПРЯМКИ ВИКОРИСТАННЯ КВАДРОКОПТЕРУ «DJI MAVIC PRO 2 ENTERPRISE» У ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

З моменту своєї появи в 2006 році [1] такі сучасні безпілотні літальні апарати як квадрокоптери знаходять все ширше використання у майже всіх сферах діяльності людини, суспільства та країни, таких як, журналістика, медицина, охорона, кіно тощо. На сьогодні квадрокоптери також використовуються у діяльності правоохоронних органів, у тому числі в Національній поліції України. Так, наприклад, в структурі Департаменту патрульної поліції Національної поліції України діє відділ аеропідтримки Управління моніторингу та аналітичного забезпечення, що знаходиться у місті Дніпро.

В жовтні 2018 року в Україні було презентовано нову модель квадракоптеру компанії «DJI» – «Mavic Pro 2 Enterprise», який позиціонується розробником як квадрокоптер, що був розроблений для потреб промисловості та публічної безпеки.

Технічні характеристики «DJI Mavic Pro 2 Enterprise» наступні: час польоту до 31 хвилини, максимальна швидкість (в безвітряну погоду) 72 км/год, дальність передачі сигналу до 8 кілометрів, 12-мегапіксельна камера з CMOS-матрицею на 1/2.3, максимальна роздільна здатність відео 3840 x 2160 при 30 fps, максимальний бітрейт відео 100 Мбіт/с, OcuSync 2.0, стабілізація камери по трьох осях, 2-х кратний оптичний зум, 3-х цифровий зум, виявлення перешкод в шести напрямках, вбудована пам'ять 24 гігабайти, вага 905 грам.

Окрім того під час польоту «Mavic Pro 2 Enterprise» показує і записує свої GPS координати, фіксує час і дату передачі зображення на пульт пілота коптера. Всі дані надійно зберігаються в додатку «DJI Pilot». Щоб отримати доступ до нього та інших функцій, досить ввести особистий пароль. Цей спосіб входу забезпечує безпечний доступ до вбудованої пам'яті дрона, таким чином запобігаючи витоку конфіденційної інформації.

На верхній частині квадрокоптеру знаходиться невеликий майданчик з отворами для гвинтів і інтерфейсним роз'ємом microUSB для підключення змінних модулів. На сьогодні доступні три таких модулі: гучномовець «M2E Speaker», проблисковий маяк «M2E Beacon» і портативний прожектор «M2E Spotlight».

Детальніше розглянемо напрямки використання кожного із модулів.

У *гучномовця «M2E Speaker»*, який має потужність 100 Дб, можна змінювати його направленість за допомогою спеціального шарніра – вниз або вперед. Також в нього є два режими роботи: відтворення записаного аудіотрека і відтворення збереженого раніше файлу.

У першому режимі можна записати голосове повідомлення до 60 секунд за допомогою смартфона і мобільного застосування «DJI Pilot». Після синхронізації з коптером цей аудіофайл програватиметься через динамік. Залишиться тільки налаштувати гучність.

У другому режимі через гучномовець програються заздалегідь записані на смартфоні аудіофайли (всього можна запам'ятати до 10 треків). Трек можна поставити на повтор або програти один раз. Час польоту дрона з включеним гучномовцем становить 25 хвилин з урахуванням безвітряної погоди.

Проблисковий маяк «M2E Beacon» може бути використаний під час пошуку в лісовий смузі людей, наприклад, що зникли або переховуються.

Коптер можна запустити над лісовим масивом з проблисковим маячком, відшукати зниклих і, або відвести їх у безпечне місце, або надати візуальний орієнтир для інших учасників пошукової групи, в залежності від ситуації. В налаштуваннях можна або активувати «M2E Beacon», або вимкнути його. Час польоту з включеним маяком становить 27 хвилин з урахуванням безвітряної погоди.

Портативний прожектор «M2E Spotlight» може бути використаний під час проведення пошуково-рятувальних операцій в нічний час, в якості портативного літаючого ліхтаря при розборі завалів, а при спільному використанні з режимом «Active Track 2.0» – оператор може під підсвічувати дорогу [2].

У відповідності до ст. 2 Закону України «Про Національну поліцію» до завдань української поліції відносяться:

«1) забезпечення публічної безпеки і порядку;

2) охорони прав і свобод людини, а також інтересів суспільства і держави;

3) протидії злочинності;

4) надання в межах, визначених законом, послуг з допомоги особам, які з особистих, економічних, соціальних причин або внаслідок надзвичайних ситуацій потребують такої допомоги» [3].

До напрямків використання квадрокоптеру «DJI Mavic Pro 2 Enterprise» у діяльності Національної поліції України можна віднести:

1) протидія злочинності:

– для проведення візуальної розвідки з метою виявлення можливих загроз для людей та правоохоронців, наприклад, виявлення місця

перебування зловмисників на певній території чи в будівлі, встановлення чи озброєні вони та чим саме [4, с. 211];

– виявлення місць відстою вантажівок з товаром, що був незаконно завезений на територію України, або обіг якого заборонений в Україні;

– виявлення місць незаконних посівів нарковмісних рослин;

– передача відеосигналу та фотографій для подальшого розпізнавання осіб і номерних знаків автомобілів, які перебувають у розшуку;

– дистанційне обстеження підозрілих предметів (наприклад, пакетів або сумок) з метою проведення первинної оцінки щодо належності цих предметів до вибухових пристроїв;

2) в пошуково-рятувальних операціях, у тому числі в нічний час, наприклад, для пошуку осіб:

– які загубились;

– постраждали в наслідок аварій техногенного чи природного характеру;

3) під час забезпечення публічної безпеки та порядку:

– у місцях масового скупчення людей, наприклад, для виявлення та своєчасного припинення протиправних дій шляхом звернення через гучномовець до осіб, які вчинять протиправні дії з вимогою припинити правопорушення;

– на автошляхах та автомагістралях для виявлення та аналізу дорожньо-транспортних пригод, шляхів проїзду до місця події.

Наведений перелік не є вичерпним.

Висновки. В останні роки безпілотна авіація активно розвивається, безпілотні апарати отримують нові технічні характеристики та можливості. Такі летальні апарати можуть та повинні застосовуватися в правоохоронних органах, у тому числі у Національній поліції України для покращення можливостей поліцейських та рівня виконання завдань покладених на поліцію.

Список бібліографічних посилань:

1. Шевчук А. Когда изобрели квадрокоптер: история квадрокоптеров с 2006 и по сегодня // MOYO – свой в мире интернет-покупок. 20.08.2018 11:00. URL: https://www.moyo.ua/news/kogda_izobreli_kvadrokopter_istoriya_kvadrokopterov_s_2006_i_po_segodnya.html (дата звернення: 28.11.2018).

2. Ваш новый союзник в небе Mavic 2 Enterprise // Хабр. 29 октября 2018 в 19:48. URL: https://habr.com/post/428149/ (дата звернення: 28.11.2018).

3. Про Національну поліцію : Закон України від 02.07.2015 № 580-VIII, в редакції від 25.11.2018 // БД «Законодавство України» / ВР України. URL: http://zakon.rada.gov.ua/laws/show/580-19 (дата звернення: 28.11.2018).

4. Хворостенко М.М. Особливості використання квадрокоптерів під час охорони публічної безпеки та порядку // Актуальні проблеми сучасної науки і правоохоронної діяльності : тези доп. учасників XXIV наук.-практ. конф. курсантів та студентів (м. Харків, 17 трав. 2017 р.) / МВС України, Харків. нац. ун-т внутр. справ, Наук. т-во студентів, курсантів, слухачів, аспірантів, ад'юнктів, докторантів і молодих вчених. Харків, 2017. С. 210-211. URL:

http://univd.edu.ua/general/publishing/konf/17_05_2017/pdf/112.pdf (дата звернення: 28.11.2018).

УДК 65.012.8 + 004

ВІКТОРІЯ ОЛЕКСАНДРІВНА КОВТУН
курсант 1 курсу факульту № 4 Харківського національного університету внутрішніх справ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В СУСПІЛЬСТВІ

Інформаційні технології (ІТ) – процеси, методи пошуку, збору, зберігання, обробки, надання, поширення інформації та способи здійснення таких процесів і методів; прийоми, способи і методи застосування засобів обчислювальної техніки при виконанні функцій збору, зберігання, обробки, передачі і використання даних; ресурси, необхідні для збору, обробки, зберігання і розповсюдження інформації.

Роль ІТ у розвитку суспільства полягає в прискоренні процесів отримання, поширення та використання суспільством нових знань. Головною функцією ІТ є розробка методів і засобів опрацювання даних та їхнє використання в різних галузях людської діяльності. Сучасні інформаційні технології стають одним з найбільш прибуткових та швидко зростаючих секторів економіки. Інформація стала важливим виробничим і комерційним ресурсом.

Інформаційні технології дозволяють активізувати й ефективно використовувати інформаційні ресурси суспільства, що заощаджує інші види ресурсів. ІТ раніше були засобом підвищення персональної продуктивності співробітників, а сьогодні стають силою, яка допомагає компанії отримати і зберегти переваги в конкурентній боротьбі.

Сучасні технології впливають не тільки на функціонування окремих компаній, але і на економіку в цілому. Вони перетворюються в соціальне явище, яке визначає, як виглядає суспільство в світовому масштабі. ІТ забезпечують інформаційну взаємодію людей, що сприяє поширенню масової інформації. Вони швидко асимілюються культурою суспільства, знімають багато соціальних, побутових та виробничих проблем, розширюють внутрішні та міжнародні економічні та культурні зв'язки, впливають на міграцію населення у світі.

Розширення застосування мережі Інтернет. З моменту створення персонального комп'ютера ніщо так не вразило комп'ютерний світ, як широке поширення мережі Інтернет та служби World Wide Web (всесвітньої павутини). Нові технології принесли в одноманітний світ тексту звук, відео і мультиплікацію. Хоча саму мережу важко назвати чимось революційним (вона існує вже понад 30 років), в останні роки зросла не тільки інтенсивність її використання, а й число послуг, що надаються.

Розвиток електронного бізнесу. У зв’язку з активним підключенням споживачів до Інтернету ділові люди також шукають виходу в мережу. Банки пропонують послуги в електронній формі, при яких фізичні особи зможуть проводити банківські операції в режимі on-line, не приходячи для цього в банк. 24 години на добу працюють електронні магазини, реселлери в Інтернеті укладають угоди, а виробники вважають цю мережу простим і зручним способом зв'язку з постачальниками і споживачами.

Наявність великої кількості промислово функціонуючих баз даних, що містять інформацію практично по всім видам діяльності суспільства. Створені технології, що забезпечують інтерактивний доступ масового користувача до цих інформаційних ресурсів.

Розширення функціональних можливостей інформаційних систем, що забезпечують паралельну одночасну обробку баз даних з різноманітною структурою даних, мультиоб'єктних документів, гіперсередовищ, в тому числі реалізують технології створення і ведення гіпертекстових баз даних.

Зближення ринків побутової та комп'ютерної техніки. Це сталося завдяки зміні форми запису відео та звуку з аналогової на цифрову. В основі роботи найпростішого програвача CD і складного комп'ютера лежить один принцип - обробка цифрового сигналу.

Локальні безпровідні мережі. Розширення меж офісу. Можливість мати комп'ютер завжди під рукою – життєво важливо для сучасної людини. На розширення меж офісу дуже вплинули успіхи в розвитку безпровідних технологій, особливо факсів і модемів.

У XXI столітті освічена людина - це людина, яка добре володіє інформаційними технологіями. Адже зараз діяльність людей усе більше залежить від їх інформованості та здатності ефективно використовувати інформацію. Сучасний фахівець будь-якого профілю в інформаційних потоках повинен вміти отримувати, обробляти і використовувати інформацію за допомогою комп'ютерів і інших засобів. Основну роль незабаром буде грати система поширення, зберігання та обробки інформації. Техніка, завдяки якій багатьом людям стало набагато легше - сучасні інформаційні технології.

Список бібліографічних посилань

1. http://sophus.at.ua/publ/2013_12_19_20_kampodilsk/sekcija_7_2013_12_19_20/informacijni_tekhnologiji_v_suchasnomu_sviti/49-1-0-863
2. https://ukrbukva.net/61690-Informacionnye-tehnologii-v-obshestve-Ponyatie-informacionnogo-obshestva.html
3. https://stud.com.ua/86670/informatika/informatsiyni_tehnologiyi_suspilstvi_stolittya
4. https://mozok.click/731-nformacyn-tehnologyi-u-susplstv.html
5. https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D1%96_%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D1%96%D1%97
6. https://sites.google.com/site/rgpuktnoscience/Home/lec/lec1

УДК 364.04:314.18
ВІТАЛІЙ ОЛЕГОВИЧ НАЙДА
курсант 3 курсу факультету № 1
Харківського національного університету внутрішніх справ
ПЕТРО СЕРГІЙОВИЧ КЛІМУШИН
кандидат технічних наук, доцент,
доцент кафедри інформаційних технологій
Харківського національного університету внутрішніх справ

ВІРТУАЛЬНЕ ПРАВО ЯК НОВИЙ НАПРЯМОК ЮРИДИЧНИХ ДОСЛІДЖЕНЬ

Віртуальне право - новий напрямок юридичних досліджень, предметом якого є правові проблеми, що виникають з приводу віртуальних світів. Останні ж являють собою принципово новий соціально-комунікативний феномен, матеріальну основу якого складають сучасні інформаційні технології.

Актуальні тенденції розвитку віртуального світу як створеного програмними засобами віртуального середовища, призначеного для взаємодії між користувачами, породжують значний розвиток ігрової за своєю природою взаємодії і реальні економічні відносини між користувачами.

Основною правовою проблемою, пов'язаною з цим, є сама можливість і межі застосування до віртуального світу відносин права реального світу. З проблемою можливості застосування реального права до віртуальних відносин пов'язана правова невизначеність терміна «комп’ютерна гра», а також невизначеність меж, де закінчуються віртуальні правові наслідки і настають реальні. Один із запропонованих зарубіжними авторами підходів полягає в «тесті магічного кола», який передбачає необхідність з'ясування того, чи віддавав звіт користувач у тому, що його віртуальні дії мають реальні наслідки. До речі, дана проблема має і зворотну сторону - комерціалізація віртуальних світів може зашкодити їм самим як різновиду сучасного інтерактивного мистецтва. Деякі автори в зв'язку з цим пропонують на законодавчому рівні закріпити поділ віртуальних світів на ті, що мають і не мають комерційної складової.

З межами застосування реального права до віртуального світу пов’язано безліч конкретних галузевих проблем.

Наприклад, проблема застосовного права та юрисдикції. Велика частина віртуальних світів, як і інші інтернет-феномени, принципово включають в себе іноземний елемент - брати участь у віртуальному світі може безліч користувачів з різних країн світу, але ні в теорії, ні на практиці немає усталеної думки, в якому порядку і на підставі якого права повинні вирішуватися спори як між окремими користувачами, так і між користувачами і компаніями, які забезпечують доступ до віртуального світу.

Інша галузева проблема, пов'язана з віртуальними правовідносинами, - це проблема «віртуальної власності». Згідно багатьох призначених для

користувача угод, віртуальні об'єкти представляють собою об'єкт інтелектуальних прав, який учасник віртуального світу використовує на підставі невиключної ліцензії. Даний підхід є розумним в світлі діючих норм права інтелектуальної власності, однак він може вступати в протиріччя з економічною основою цих відносин. Віртуальні предмети все частіше стають предметом угод, а за своїм змістом представляють собою саме угоди купівлі-продажу.

Цими проблемами віртуальне право не вичерпується, оскільки через віртуальні світи відображається майже весь спектр проблем інтернет-права. Але, більш того, ті віртуальні світи, яким властива віртуальна соціальна реальність, можуть представляти інтерес не тільки для галузевих юридичних наук, а й для теорії і соціології права, виступаючи в якості моделей реальних відносин або, можливо, простору для соціального експерименту .

Примітно, що у світі інтерес до проблем віртуального права зростає і знаходить своє відображення в різних професійних асоціаціях юристів. Так, наприклад, секція з правової науки і технології Американської асоціації адвокатів включає в себе комітет з віртуальних світів і онлайн-ігор.

Якщо розвиток інформаційно-комунікаційних технологій та індустрії електронних розваг продовжиться в нинішньому напрямку, актуальність вивчення проблем віртуального права буде тільки зростати.

УДК 681.3.06

ПОЛІНА ІВАНІВНА ПОПОВСЬКА
курсант 3 курсу факультету №4 Харківського національного університету внутрішніх справ

ОСНОВИ ЗАСТОСУВАННЯ ЗАСОБІВ ЗВУКОЗАПИСУ В ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ

Сьогодні вже ні для кого не таємниця, що інформаційні технології є невід'ємною частиною в діяльності сучасної поліції. Неодмінною умовою підвищення ефективності управлінської праці є інформаційні технології, що володіють гнучкістю, мобільністю і адаптивністю до зовнішніх впливів. Інформаційні технології передбачають вміння грамотне працювати з інформацією та обчислювальною технікою.

Спеціальні технічні засоби (СТЗ) можна класифікувати відповідно до слідчої, оперативно-розшукової та адміністративної діяльності органів внутрішніх справ (спеціальні технічні засоби загального призначення).

Під час розслідування злочинів СТЗ використовуються гласно для збирання і дослідження доказів. Технічні засоби, прилади та прийоми охоплюються поняттям ”криміналістична техніка”. Ці питання розглядалися також при застосуванні знарядь і приладів пошукової техніки [2, с. 76], приладів спостереження [3, с. 44]. Застосування криміналістичної техніки регулюється нормами кримінально-процесуального закону.

Використання звукозапису в роботі поліції, має велике значення при проведенні слідчих дій і оперативно-розшукових заходів, пов'язаних зі збиранням і фіксацією звукової інформації. Звукозапис може бути використаною для ідентифікації особи за голосом, для проведення її впізнання за голосом, для перевірки за обліком фонограм. Для ефективної роботи слідчих і оперативних підрозділів по розкриттю злочинів застосовуються засоби звукозапису та оперативного прослуховування, що дозволяє з великою точністю й повнотою фіксувати людську мову та іншу звукову інформацію при наявності спеціальних технічних, криміналістичних засобів і методів.

Стосовно оперативно-розшукових заходів звукозапис може використовується негласно, наприклад: коли йдуть переговори між замовником і виконавцем злочину. Фонограми можуть в опечатаному вигляді на відповідному носії зберігається при справі. Суд, дослідивши джерела інформації, отримані із застосуванням спеціальних технічних засобів, дає їм оцінку та можливість їх використання як доказів. В оперативно-розшуковій діяльності засоби звукозапису використовуються для отримання інформації (гласно і негласно).

Оперативне використання звукозапису регламентується: законами України «Про національну поліцію», «Про оперативно-розшукову діяльність», Кримінально процесуальним кодексом України (ст.252, 256, 260, 266, 267, 269, 270), наказами МВС України.

Використання засобів звукозапису в оперативно-розшуковій діяльності документально оформляється: *довідкою* – оперативним працівником за наслідками проведеної роботи, *актом, планом, рапортом***,** якщо технічний засіб застосовується оперативним працівником самостійно або із залученням працівників інших служб.

В слідчій діяльності засоби звукозапису переважно використовуються для фіксації наступних процесуальних дій: 1) при огляді; 2) при слідчому експерименті; 3) при обшуку; 4) при допитах.

У випадку фіксування процесуальної дії під час досудового розслідування за допомогою технічних засобів про це зазначається у протоколі (стаття 104. КПК України) [1].

При проведенні слідчих дій з застосуванням звукозапису про це повідомляються всі учасники слідчої дії до її початку. Фонограма повинна містити відомості, зазначені у частині 1 статті 85 цього Кодексу, та відбивати весь хід слідчої дії. Повторення спеціально для звукозапису будь-якої частини слідчої дії в ході її проведення не дозволяється (стаття 85-1. КПК України) [1].

Перед закінченням слідчої дії звукозапис повністю відтворюється учасникам цієї дії (стаття 85-1. КПК України) [1].

При пред'явленні учасникам процесу матеріалів справи у зв'язку з закінченням досудового розслідування звукозапис відтворюється обвинуваченому і його захиснику, а в разі клопотання – і іншим учасникам

процесу. Фонограма в опечатаному вигляді зберігається при справі (стаття 85-1. КПК України) [1].

Як висновок можна виділити, що звукозаписуючі пристрої широко використовують у попередженні злочинів та профілактичній діяльності органів дізнання, слідства й суду. Значну роль вони відіграють в адміністративно-профілактичній діяльності, попередженні проступків і правопорушень. Основною метою використання звукозапису при розслідуванні є забезпечення додаткової наочно-звукової фіксації ходу окремих слідчих дій. Особливо таких слідчих дій, як допит, очна ставка, перевірка показань на місці, пред'явлення для впізнання. У тактиці проведення зазначених слідчих дій визначені ті ситуації, коли доцільно використання звукозапису в якості допоміжного засобу їх фіксації.

Список бібліографічних посилань:

1. Кримінальний процесуальний кодекс України. Кодекс кримінальний процесуальний від 13.04.2012 № 4651-VI. Редакція: 18.10.2018.

2. Гончар В. К., Золотар О. В. Знаряддя та прилади пошукової техніки: Навч. посіб. Київ: Нац. акад. внутр. справ України, 2001.

3. Гончар В. К., Золотар О. В. Прилади спостереження в екстремальних умовах: Навч. посіб. Київ: Нац. акад. внутр. справ України, 2003.

УДК 681.3.06

АННА ОЛЕКСАНДРІВНА ОСТРОВЕРХОВА
курсант 3 курсу факультету № 4
Харківського національного університету внутрішніх справ

АНАЛІЗ ПОПУЛЯРНИХ ПРОГРАМНО-АПАРАТНИХ ДЕВАЙСІВ ТА ГАДЖЕТІВ В ДІЯЛЬНОСТІ ПОЛІЦЕЙСЬКИХ

Стрімкий розвиток інформаційних технологій поступово трансформує світ. Усі сфери суспільного життя та виробництва модернізуються за рахунок використання електронно-обчислювальних машин. Також для забезпечення ефективної діяльності Національної поліції України треба використовувати якомога більше сучасних програмно-апаратних девайсів та гаджетів спеціального призначення.

Девайс (device) – це самостійне, багатофункціональний програмно-апаратний пристрій, яке використовується в багатьох областях, призначене для виконання приватного, спеціального завдання (наприклад комп'ютер, ноутбук, планшет, смартфон, бортовій комп’ютер до автомобілю патрульної служби).

Гаджет (gadget) – це програмно-апаратний пристрій, створений в допоміжних цілях, для роботи якого можуть знадобитися додаткові пристрої. (електронній паспорт, електронні браслети, окуляри віртуальної реальності, натільна камера, розумні відеокамери, квадрокоптер).

Рівень оснащеності поліції щороку зростає. Так в Україні впроваджують такі нові інструменти забезпечення діяльності: безготівкові термінали для сплати штрафів, бортові комп'ютерами до автомобілю патрульної служби, натільні камери та квадрокоптери. За словами міністра внутрішніх справ, основні переваги цих нововведень є скорочення часу заповнення протоколів, підвищення ефективності роботи поліції і мінімізації ризиків корупції. Для цього вводиться система "електронний протокол", що також є інструментом моніторингу добропорядності роботи поліцейського.

Встановлення бортових комп'ютерів до автомобілю патрульної служби дозволить поліцейським підключатись до бази даних та отримувати інформацію про вчинення раніше правопорушення та винесені рішення, аби правоохоронці одразу могли побачити всю історію конкретного автомобіля.

Портативні мобільні принтери друкуватимуть протоколи та виписки штрафів, задля уникнення розбіжностей та конфліктів між водієм та поліцейським.

Використання квадрокоптерів допомагає у потенційно небезпечних для ситуаціях (затримання озброєних осіб, рятувальні місії, патрулювання кордонів, розшук безвісно зниклих людей тощо), не ризикуючи життям та здоров'ям правоохоронців.

Сучасні іноземні департаменти поліції мають безліч пристроїв та інструментів, які можуть революціонізувати правоохоронні органи та сприяти підтримці громадської безпеки.

Носіння натільної камери, яка фіксує всі дії патрульного та громадянина набула широкого поширення в США за останній рік, після низки конфліктів між поліцейськими та жителями.

Сучасні комп'ютерні системи тепер можуть допомагати працівникам правоохоронних органів ефективно прогнозувати, де відбуваються злочини на основі геолокації.

Наприклад, державна поліція штату Пенсільванії нещодавно розробила технологію, яка аналізує тенденції вчинення злочинів та допомагає виявляти ймовірне вчинення злочинів.

Співробітники поліції використовують електронні портативні сканери, щоб миттєво відскановувати відбитки пальців та ідентифікувати осіб, які мають причетність до вчинення зареєстрованих злочинів. Завдяки миттєвому доступу до бази даних ці пристрої дають змогу пришвидшити отримання інформації про осіб.

До перспективних гаджетів застосування в Україні належить віртуальні (розумні) окуляри. Окуляри можуть робити фотографії, знімати відео в HD-якості і відображати деякі елементи на лінзах за допомогою технології доповненої реальності. Офіцери поліції в основному користуються функцією розпізнавання осіб, щоб проводити перевірки і звіряти документи.

Говорячи про запозичення досвіду зарубіжних країн в застосуванні супутникових навігаційних систем в першу чергу необхідно звернути увагу на практику застосування на Україні таких гаджетів як електронні браслети для стеження за обвинуваченими / підозрюваними.

Таким чином, аналіз популярних програмно-апаратних девайсів та гаджетів в діяльності поліцейських показав, що їх впровадження здійснюється відповідно до національних законодавств, направлено на забезпечення правопорядку з дотриманням конституційних прав громадян та підвищення ефективності діяльності поліцейських. Аналіз дозволив виділити найбільш актуальні для впровадження в України програмно-апаратних засобів: натільні відеокамери, розумні відеокамері, квадрокоптери, розумні окуляри з функцією розпізнавання особистості, електронні портативні сканери відбитків пальців та ідентифікації осіб.

УДК 007[732.214]
ЯРОСЛАВ АНДРІЙОВИЧ ЧЕРКАШЕНКО
рядовий поліції курсант 2 курсу факультету № 4 Харківського національного університету внутрішніх справ

КІБЕРВІЙНА ТА ІНФОРМАЦІЙНИЙ ВПЛИВ НА СУСПІЛЬСТВО

В умовах глобальної і тотальної інформатизації, коли суспільство стало залежним від інформаційних систем, політичні і військові еліти стали застосовувати віртуальний вплив на людей, приховано, а інколи й відкрито. Настав час війни не на полі бою, а в мережі Інтернет ,та витрати на такий засіб бою потребується менш. При цьому ефективно проводити дезінформацію компаній, виявляти та контролювати громадську думку, направляти соціальні групи на певні дії дозволяють соціальні мережі.

Недооцінювання та нехтування тою чи іншою державою питань власної кібербезпеки й інформаційного домінування може спричинити не лише суттєві матеріальні збитки через втрату або спотворення стратегічної важливої інформації, а й можливі техногенні катастрофи, збитки цивільної, фінансової та військової інфраструктури аж до втрати суверенітету держави.

Мережева війна – це спосіб ведення конфліктів, коли її учасники застосовують мережеві форми організації, доктрини, стратегії та технології, пристосовані до сучасної інформаційної доби.

З іншого ж боку на сьогоднішній день більшість держав вже приділяють захисту від кібервійни належну увагу: виділяють необхідні кошти для організації систем захисту і підтримання спеціальні підрозділи, основним завданням яких є вдосконалення кібербезпеки країни та захисту від нападів.

[2] У кібервійні часто неможливо визначити не тільки учасників, час її початку і завершення, а й важко довести у багатьох випадках сам факт застосування руйнівної кіберзброї, не кажучи вже про шпигунське програмне забезпечення. За своїми наслідками застосування кіберзброї під час наступальних операцій в електромагнітному спектрі можна порівняти із втратами від застосування зброї масового ураження. Зокрема, використання кіберзброї може бути замасковано під техногенні катастрофи чи системні збої в системі комп’ютерних мереж і сервісів тощо. Так, прикладом, 23 грудня

2015 року за допомогою троянської програми «Black Energy» російські зловмисники атакували комп'ютерні системи управління в диспетчерській «Прикарпаттяобленерго» та вимкнули понад 30 підстанцій, залишивши 230 тисяч мешканців без світла на 1-6 годин. Ця атака стала першою у світі підтвердженою кібератакою спрямованою на виведення з ладу енергосистеми.

[1] Також з одного боку, існує багато спроб звести інформаційну війну до проблем комп'ютерних технологій, тобто до реалізації можливостей технологічних засобів передавання, опрацювання та використання інформації, а з іншого – до психологічної війни, тобто до використання засобів впливу на людину.

Нині в нашій країні інформаційні відносини та питання гарантування інформаційної та кібернетичної безпеки врегульовуються законами України «Про основи національної безпеки України».

Але проблема в тому, що якщо окремі держави не будуть обмінюватися інформацією, то інформаційна безпека не буде кращим виглядом підніматися в рівні захищеності та здобуття навичок запобігання кібератак, якщо буде виявлення в момент різкого виявлення загрози інформаційного напрямку.

Незважаючи на глобальний характер кібератак, на сьогодні відсутнє єдине міжнародно-правове визначення поняття кіберзлочинності, інформаційної війни та кібервіни. Немає міжнародно-правового механізму регулювання відносин у кіберпросторі.

Перспективи зміни системи міжнародної безпеки досить туманні, проте вже зрозуміло, що більшість інститутів і загальноприйнятих механізмів зараз малоефективні. Надалі в умовах розбудови глобального інформаційного суспільства можливим є тільки спільне підтримання балансу у сфері міжнародної безпеки на базі міждержавних союзів. Для безпеки кіберпростору нашої держави потрібно узгоджувати та поєднувати національну та міжнародну стратегію кіберзахисту у рамках спільної безпеки й оборонної політики ЄС, а також інтенсифікувати співпрацю України та НАТО, встановлення балансу між інформаційною безпекою і повагою приватного життя, створення конфіденційних механізмів обміну інформацією, встановлення основних вимог до кібербезпеки, відповідальності за кіберзлочинність, зміцнення програм освіти і професійної підготовки, підвищення обізнаності громадськості з питань кібербезпеки в нашій державі.

Список використаних джерел:

1. Попов.М.О., Лук'янець А.Г. До забезпечення воєнної безпеки в умовах загрози інформаційної війни. Наука й оборона.1999,№2. С.37–43.

2. Размєтаєва Ю.С. Кібервійна: загальнотеоретичні аспекти. Вісник АМСУ. Серія «Право». 2015, №1(14). С.17–22.

УДК 623.746+351.74
ЛОЛІТА АНДРІЇВНА МАГДА
курсант 2 курсу факультету №4 Харківського національного університету внутрішніх справ

ВИКОРИСТАННЯ ОКУЛЯРІВ GOOGLE GLASS 3.0 В ПІДРОЗДІЛАХ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ

В наші дні інформаційні технології відіграють важливу роль, і значення інформації у всіх сферах людської діяльності на сучасному етапі постійно зростає. Цей аспект пов’язаний зі зміною соціально-економічної сфери суспільства, появи нових досягнень в області технологій. Під впливом науково-технічного прогресу повсюдно впроваджуються нові пристрої, які надають унікальні можливості для швидкого і ефективного розвитку як держави в цілому, так і окремо взятої особистості.

Сьогодні серед першочергових потреб підрозділів Національної поліції, поряд з формуванням кадрового потенціалу стоїть необхідність впровадження в службовій діяльності нових технічних засобів, головною ціллю цих модернізацій є створення сучасної та ефективної правоохоронної системи.

Таким пристроєм можуть стати інноваційні окуляри Google Glass 3.0 для iOS / Android смартфонів, котрі проектують зображення на прозорий дисплей, роблять фото, знімають HD-відео, показують повідомлення і пошту.

Окуляри проектують перед користувачем віртуальний екран в 25" на відстані 2,5 метра з дозволом 640x360 пікселів. За допомогою вбудованої відеокамери в 5 Мп знімають якісне HD відео і роблять фотознімки, мають голосове управління (близько 15 команд) і сенсорну панель. Для того, щоб, наприклад, зробити фото, досить моргнути оком. Завдяки вбудованому GPS-приймача, Google Glass 3.0 здатні визначити Ваше місце розташування, швидкість пересування і прокласти маршрут в незнайомому місті. Якщо буде потрібна інформація з інтернету, досить адресувати своє питання Google Glass і негайно отримаєте відповідь. Окуляри, навіть, можуть здійснювати переклад на різні мови світу.

Спеціально для окулярів розробляється або вже створено велику кількість всіляких додатків. Наприклад, додаток для безпечного водіння DriveSafe4Glass, яке попередить водія, якщо той засне за кермом.

Технічні характеристики: операційна система: Android 4.0.3; сумісність: iOS / Android пристрої; дисплей: розмір 25 "на відстані 2,5 метра з дозволом 640x360 пікселів; камера: відео 720p HD, фото 5 Мп; процесор: OMAP 4430, з частотою 1.2 GHz; пам'ять: оперативна 1Гб, загальна 16 Гб; підключення: Wi-FiI EEE 802.11b / g, Bluetooth 4.0; особливості: вбудований GPS-модуль, акселерометр, датчик носіння окулярів.

Для співробітників поліції даний пристрій може стати неабиякою знахідкою. Так поліцейському не буде потрібно перевіряти документи, що може викликати небажану реакцію підозрюваного, а буде достатньо перевірити наявність фотографії тієї чи іншої людини в базі даних поліції. А

оригінал завжди можна отримати за допомогою вбудованої в Google Glass камери. Крім того, окуляри дозволять здійснювати стеження за злочинцем, не привертаючи уваги до поліцейського, а також звільняючи його руки для застосування зброї або рукопашної сутички. Вони дають можливість постійно стежити за зображеннями з вуличних відеокамер, бачити переміщення співробітників, користуватися оглядовими програмами Street View, робити миттєві фотознімки, коли це необхідно, реєструвати час скоєння правопорушень, обмінюватися даними з іншими патрулями.

Також є можливість розробки та спеціальних додатків для органів правопорядку: для швидкого розпізнавання особистості, отримання даних про попередні правопорушення затриманих людей, складання електронних протоколів і т.д.

Але все ж таки виникає ряд проблем стосовно використання даних пристроїв у підрозділах Національної поліції.

По-перше це досить висока вартість, враховуючи теперішній курс долара і воєнний стан.

По-друге це необхідність встановити правові основи використання спеціальної техніки, що визначає допустимість використання або регламентує організацію, порядок, умови, способи та результати використання технічних засобів.

І по-третє це досить крихка конструкція і необхідно навчити особовий склад користуватися окулярами.

Отже, підсумовуючи вищесказане, слід відзначити, що перспективні інформаційні технології забезпечують новий рівень передачі, трансформації та аккумуляції інформації. Наша країна ще не готова до нововведень, стосовно використання окулярів. Але все ж таки, сподіваємося, що в майбутньому наша держава зможе забезпечити правоохоронні органи всією необхідною технікою.

Для нотаток

Для нотаток

Наукове видання

ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ДІЯЛЬНОСТІ НПУ

Матеріали
Науково-практичного семінару

м. Харків, 21 грудня 2018 року

ВИДАНО В АВТОСЬКІЙ РЕДАКЦІЇ

Відп. за випуск В.Є. Рог

Підписано до друку 17.12.2018 р. Формат 60х84/16. Папір офсетний.
Гарнітура Times ET. Ум. друк. арк. 5,7. Наклад 100 пр. Зам. № 1217/4-18.

Надруковано з готового оригінал-макету у друкарні ФОП В. В. Петров
Єдиний державний реєстр юридичних осіб та фізичних осіб-підприємців.
Запис № 24800000000106167 від 08.01.2009 р.
61144, м. Харків, вул. Гв. Широнінців, 79в, к. 137, тел. (057) 78-17-137.
e-mail:bookfabrik@mail.ua